Sicherheitsreferenzhandbuch




# Steuerungssysteme GuardLogix 5570

Bestellnummern 1756-L71S, 1756-L72S, 1756-L73S, 1756-L73SXT, 1756-L7SP, 1756-L7SPXT, 1756-L72EROMS,
Studio 5000 Logix Designer-Anwendungen









Übersetzung der Originalbetriebsanleitung

Allen-Bradley • Rockwell Software



## Wichtige Hinweise für den Anwender

Lesen Sie die in diesem Dokument und in den im Abschnitt „Weitere Informationsquellen“ aufgeführten Dokumenten enthaltenen Informationen, bevor Sie dieses Produkt installieren, konfigurieren, bedienen oder warten. Anwender müssen sich neben den Bestimmungen aller anwendbaren Vorschriften, Gesetze und Normen zusätzlich mit den Installations- und Verdrahtungsanweisungen vertraut machen.

Arbeiten im Rahmen der Installation, Anpassung, Inbetriebnahme, Verwendung, Montage, Demontage oder Instandhaltung dürfen nur durch ausreichend geschulte Mitarbeiter und in Übereinstimmung mit den anwendbaren Ausführungsvorschriften vorgenommen werden.

Wenn dieses Produkt nicht gemäß den Anweisungen des Herstellers verwendet wird, können die Schutzfunktionen des Produkts möglicherweise beeinträchtigt sein.

Rockwell Automation ist in keinem Fall verantwortlich oder haftbar für indirekte Schäden oder Folgeschäden, die durch den Einsatz oder die Anwendung dieses Geräts entstehen.

Die in diesem Handbuch aufgeführten Beispiele und Abbildungen dienen ausschließlich der Veranschaulichung. Aufgrund der unterschiedlichen Anforderungen der jeweiligen Anwendung kann Rockwell Automation keine Verantwortung oder Haftung für den tatsächlichen Einsatz der Produkte auf der Grundlage dieser Beispiele und Abbildungen übernehmen.

Rockwell Automation übernimmt keine patentrechtliche Haftung in Bezug auf die Verwendung von Informationen, Schaltkreisen, Geräten oder Software, die in dieser Publikation beschrieben werden.

Die Vervielfältigung des Inhalts dieser Publikation, ganz oder auszugsweise, bedarf der schriftlichen Genehmigung von Rockwell Automation.

In dieser Publikation werden folgende Hinweise verwendet, um Sie auf bestimmte Sicherheitsaspekte aufmerksam zu machen.

| | |
|---|---|
|  | **WARNUNG:** Dieser Hinweis macht sie auf Vorgehensweisen und Zustände aufmerksam, die in Gefahrenbereichen zu einer Explosion und damit zu Tod, Sachschäden oder wirtschaftlichen Verlusten führen können. |
|  | **ACHTUNG:** Dieser Hinweis macht Sie auf Vorgehensweisen oder Zustände aufmerksam, die zu Verletzungen oder Tod, Sachschäden oder wirtschaftlichen Verlusten führen können. Die Achtungshinweise helfen Ihnen, eine Gefahr zu erkennen, die Gefahr zu vermeiden und die Folgen abzuschätzen. |
| **WICHTIG** | Dieser Hinweis enthält Informationen, die für den erfolgreichen Einsatz und das Verstehen des Produkts besonders wichtig sind. |

Etiketten, die am oder im Produkt angebracht sind, können auf besondere Vorsichtsmaßnahmen hinweisen.

| | |
|---|---|
|  | **STROMSCHLAGGEFAHR:** An der Außenseite oder im Inneren des Geräts, beispielsweise eines Antriebs oder Motors, kann ein Etikett dieser Art angebracht sein, um sie darauf hinzuweisen, dass möglicherweise eine gefährliche Spannung anliegt. |
|  | **VERBRENNUNGSGEFAHR:** An der Außenseite oder im Inneren des Geräts, beispielsweise eines Antriebs oder Motors, kann ein Etikett dieser Art angebracht sein, um sie darauf hinzuweisen, dass die Oberflächen möglicherweise gefährliche Temperaturen aufweisen. |
|  | **GEFAHR DER LICHTBOGENBILDUNG:** An der Außenseite oder im Inneren des Produkts, z. B. eines Motor Control Centers (MCC), angebrachte Etiketten können Anwender auf die Gefahr einer möglichen Lichtbogenbildung hinweisen. Lichtbögen können zu schweren Verletzungen oder zum Tod führen. Tragen Sie eine geeignete persönliche Schutzausrüstung (PPE). Befolgen Sie ALLE gesetzlichen Vorschriften hinsichtlich sicherer Arbeitsmethoden und persönlicher Schutzausrüstung (PPE). |

Dieses Handbuch enthält neue und aktualisierte Informationen.

## Neue und aktualisierte Informationen

In dieser Tabelle sind die Änderungen aufgeführt, die an dieser Version vorgenommen wurden.

| Thema | Seite |
|---|---|
| Verweise auf Sicherheits-E/A-Module wurden in den allgemeineren Begriff „Sicherheits-E/A-Geräte“ geändert, sofern zutreffend | Im gesamten Handbuch |
| Neue Bestellnummer 1756-L72EROMS für Armor™ GuardLogix® auf der Titelseite | Titelseite |
| Neue Informationen zu Kinetix® 5500-Servoantrieben in der Liste der Komponenten mit SIL 3-Zertifizierung | 16 |
| Neues 1756-EN2TRXT-Modul in der Liste der Kommunikationsschnittstellen-module | 23 |
| Neuer Hinweis, dass ein Projekt nicht verifiziert werden kann, wenn Kombinationen aus doppelten SNN und Netzknotenadressen vorliegen | 35 |
| Neuer Verweis auf das Benutzerhandbuch für Kinetix 5500-Servoantriebe, wenn es um Informationen zur Verwendung direkter Achssteuerungsbefehle in Sicherheitsanwendungen geht | 72 |
| Neue, aktualisierte Sicherheitsdaten (IEC 61508. Edition 2, 2010) für Guard I/O™-Module | Anhang E |
| Neue Sicherheitsdaten für 1734-IB8S-Module der Serie B und 1734-OB8S-Module der Serie B | Anhang E |
| Aktualisierte PFH-Daten für 1734-IE4S-Module | Anhang E |

# Notizen:

## Vorwort



## Kapitel 1
### Informationen zu SIL



## Kapitel 2
### GuardLogix-Steuerungssystem



## Kapitel 3
### CIP Safety-E/A für das GuardLogix-Steuerungssystem

## Informationen zu CIP Safety und zur Sicherheitsnetzwerknummer

### Kapitel 4



## Merkmale von Sicherheits-Tags, der Sicherheits-Task und von Sicherheitsprogrammen

### Kapitel 5



## Entwicklung von Sicherheitsanwendungen

### Kapitel 6

## Kapitel 7
## Überwachung des Status und Handhabung von Störungen



## Anhang A
## Sicherheitsbefehle

## Anhang B
## Sicherheits-Add-On-Befehle

## Anhang C
## Reaktionszeiten



## Anhang D
## Checklisten für GuardLogix-Sicherheitsanwendungen



## Anhang E
## Sicherheitsdaten der GuardLogix-Systeme



## Anhang F
## Software RSLogix 5000, ab Version 14, Beschreibung der Befehle für Sicherheitsanwendungen



## Anhang G
## Verwendung von 1794 FLEX I/O-Modulen und 1756 SIL 2-Eingängen und -Ausgängen mit 1756 GuardLogix-Steuerungen zur Einhaltung der EN 50156



## Glossar

## Index

Dieses Handbuch beschreibt das GuardLogix 5570-Steuerungssystem, das **baumustergeprüft** und für den Einsatz in Sicherheitsanwendungen bis einschließlich SIL CL 3 gemäß IEC 61508 und IEC 62061 sowie für den Einsatz in Sicherheitsanwendungen bis einschließlich Performance Level PLe (Kategorie 4) gemäß ISO 13849-1 zertifiziert ist.

Verwenden Sie dieses Handbuch, wenn Sie für die Entwicklung, Bedienung oder Wartung eines auf einer GuardLogix 5570-Steuerung basierenden Sicherheitssystems verantwortlich sind, das mit Studio 5000® Logix Designer ab Version 21.000 arbeitet. Sie müssen die Sicherheitskonzepte und die Anforderungen, die in diesem Handbuch vorgestellt werden, vor der Inbetriebnahme eines auf einer GuardLogix 5570-Steuerung basierenden Sicherheitssystems gelesen und verstanden haben.

Informationen zu den sicherheitstechnischen Anforderungen, die mit GuardLogix 5570-Steuerungen in RSLogix™ 5000-Projekten zusammenhängen, finden Sie im Referenzhandbuch „Steuerungssysteme GuardLogix“, Publikation 1756-RM093.

## Studio 5000-Umgebung

Studio 5000 Automation Engineering and Design Environment™ vereint Engineering- und Entwicklungselemente in einer gemeinsamen Umgebung. Das erste Element in der Studio 5000-Umgebung ist die Anwendung Logix Designer. „Logix Designer“ ist der neue Name der Software RSLogix 5000 und wird auch weiterhin das Produkt zur Programmierung von Logix5000™-Steuerungen für diskrete, Prozess-, Batch-, Achssteuerungs-, Sicherheits- und antriebsbasierte Lösungen sein.



Die Studio 5000-Umgebung bildet die Grundlage für die zukünftigen technischen Konstruktionstools und -funktionalitäten von Rockwell Automation®. Sie ist die einzige Plattform, auf der Entwickler alle Elemente ihres Steuerungssystems entwickeln.

## Verwendete Begriffe

In der folgenden Tabelle werden die in diesem Handbuch verwendeten Begriffe definiert.

**Tabelle 1 – Begriffe und Definitionen**

| Abkürzung | Vollständiger Begriff | Definition |
|---|---|---|
| 1oo2 | One Out of Two (Eins-aus-zwei-Auswertung) | Identifiziert die Architektur der programmierbaren Elektroniksteuerung. |
| CIP | Common Industrial Protocol | Ein industrielles Kommunikationsprotokoll, das von Automatisierungssystemen, die auf Logix5000 basieren, in Ethernet/IP™-, ControlNet™- und DeviceNet™-Kommunikationsnetzwerken verwendet wird. |
| CIP Safety | Common Industrial Protocol – modernes Industrieprotokoll, sicherheitszertifiziert | Für SIL 3 ausgelegte Version des CIP. |
| DC | Diagnose-Deckungsgrad | Das Verhältnis der Rate der erkannten Ausfälle zur gesamten Ausfallrate. |
| EN | Europäische Norm. | Die offizielle europäische Industrienorm. |
| GSV | Get System Value (Erhalt des Systemwerts) | Ein Befehl der Kontaktplanlogik, der spezifizierte Steuerungsstatusinformationen abruft und sie in einem Ziel-Tag ablegt. |
| PC | Personal-Computer | Computer, der als Systemschnittstelle und zur Steuerung eines Systems auf Logix-Basis über die Studio 5000-Umgebung dient. |
| PFD | Probability of Failure on Demand (Wahrscheinlichkeit eines Ausfalls bei Anforderung) | Die mittlere Wahrscheinlichkeit, dass ein System seine Designfunktion auf Anforderung nicht ausführt. |
| PFH | Probability of Failure per Hour (Wahrscheinlichkeit eines Ausfalls pro Stunde) | Die Wahrscheinlichkeit eines gefährlichen Ausfalls in einem System pro Stunde. |
| PL | Performance Level | Sicherheitsklassifizierung ISO 13849-1. |
| SNN | Sicherheitsnetzwerknummer | Eine eindeutige Nummer, die ein Sicherheitsnetzwerk oder Sicherheitsteilnetz in allen Netzwerken im Sicherheitssystem identifiziert. |
| SSV | Set System Value (Setzen des Systemwerts) | Ein Befehl der Kontaktplanlogik, der Steuerungssystemdaten festlegt. |
| -- | Standard | Objekt, Aufgabe, Tag, Programm oder Komponente in Ihrem Projekt, das bzw. die kein sicherheitsrelevantes Element ist (d. h. eine Standardsteuerung bezieht sich generisch auf eine ControlLogix®- oder eine CompactLogix™-Steuerung). |

## Weitere Informationsquellen

Die folgenden Dokumente enthalten weitere Informationen zu verwandten Produkten von Rockwell Automation.

| Quelle | Beschreibung |
|---|---|
| Benutzerhandbuch „GuardLogix 5570 Controllers User Manual“, Publikation 1756-UM022 | Informationen zu Installation, Konfiguration, Programmierung und Einsatz von GuardLogix 5570-Steuerungen in Studio 5000 Logix Designer-Projekten |
| Referenzhandbuch „Befehlssatz für GuardLogix-Sicherheitsanwendungen“, Publikation 1756-RM095 | Informationen zum Befehlssatz für GuardLogix-Sicherheitsanwendungen |
| Benutzerhandbuch „Guard I/O DeviceNet Safety Modules User Manual“, Publikation 1791DS-UM001 | Informationen zur Verwendung von Guard I/O DeviceNet-Sicherheitsmodulen |
| Benutzerhandbuch „Guard I/O EtherNet/IP-Sicherheitsmodule“, Publikation 1791ES-UM001 | Informationen zur Verwendung von Guard I/O EtherNet/IP-Sicherheitsmodulen |
| Installations- und Benutzerhandbuch „POINT Guard I/O-Sicherheitsmodule“, Publikation 1734-UM013 | Informationen zum Installieren und Verwenden von POINT Guard I/O™-Modulen |
| Kinetix 5500-Servoantriebe – Benutzerhandbuch, Publikation 2198-UM001 | Informationen zum Installieren und Verwenden von Kinetix 5500-Servoantrieben |

| Quelle | Beschreibung |
| --- | --- |
| Referenzhandbuch „Using ControlLogix in SIL 2 Applications Safety Reference Manual“, Publikation 1756-RM001 | Erläutert die Anforderungen für den Einsatz von ControlLogix-Steuerungen und einer GuardLogix-Standard-Task in SIL 2-Sicherheitssteuerungsanwendungen. |
| Referenzhandbuch „Logix5000 Steuerungen – Allgemeine Befehle“, Publikation 1756-RM003 | Informationen zum Logix5000-Befehlssatz |
| Programmierhandbuch „Logix Common Procedures Programming Manual“, Publikation 1756-PM001 | Informationen zum Programmieren von Logix5000-Steuerungen, wie z. B. dem Verwalten von Projektdateien, Organisieren von Tags, zu Programmier- und Testroutinen und zur Fehlerhandhabung |
| Logix5000 Controllers Add-On Instructions Programming Manual, Publikation 1756-PM010 | Informationen zum Erstellen und Verwenden von Standard- und Sicherheits-Add-On-Befehlen in Logix-Anwendungen |
| Benutzerhandbuch „ControlLogix-System“, Publikation 1756-UM001 | Informationen zur Verwendung von ControlLogix-Steuerungen in Nicht-Sicherheitsanwendungen |
| Benutzerhandbuch „DeviceNet Modules in Logix5000 Control Systems User Manual“, Publikation DNET-UM004 | Informationen zur Verwendung des Moduls 1756-DNB in einem Logix5000-Steuerungssystem |
| Benutzerhandbuch „EtherNet/IP Modules in Logix5000 Control Systems User Manual“, Publikation ENET-UM001 | Informationen zur Verwendung des Moduls 1756-ENBT in einem Logix5000-Steuerungssystem |
| Benutzerhandbuch „ControlNet Modules in Logix5000 Control Systems User Manual“, Publikation CNET-UM001 | Informationen zur Verwendung des Moduls 1756-CNB in Logix5000-Steuerungssystemen |
| Referenzhandbuch „Logix5000 Controllers Execution Time and Memory Use Reference Manual“, Publikation 1756-RM087 | Informationen zum Abschätzen der Ausführungszeit und Speicherbelegung der Befehle |
| Referenzhandbuch „Logix Import Export Reference Manual“, Publikation 1756-RM084 | Informationen zur Verwendung des Import/Export-Dienstprogramms Logix Designer |
| Richtlinien zur störungsfreien Verdrahtung und Erdung von industriellen Automatisierungssystemen, Publikation 1770-4.1 | Enthält allgemeine Leitlinien zur Installation eines industriellen Rockwell Automation-Systems |
| Website zu Produktzertifizierungen: http://www.ab.com | Stellt Konformitätserklärungen, Zertifikate und weitere Einzelheiten zu Zertifizierungen zur Verfügung |

Sie können weitere Publikationen unter http://www.rockwellautomation.com/literature/ anzeigen oder herunterladen. Druckexemplare der einzelnen technischen Dokumentationen erhalten Sie bei Ihrem Allen-Bradley®-Distributor oder Rockwell Automation-Ansprechpartner.

# Notizen:

# Informationen zu SIL



## SIL 3-Zertifizierung

Die GuardLogix-Steuerungssysteme der Serie 5570 sind baumustergeprüft und für den Einsatz in Sicherheitsanwendungen bis einschließlich SIL CL3 gemäß IEC 61508 und IEC 62061 sowie für den Einsatz in Sicherheitsanwendungen bis einschließlich Performance Level PLe (Kategorie 4) gemäß ISO 13849-1 zertifiziert. Die SIL-Anforderungen basieren auf den Standards, die zur Zeit der Zertifizierung gelten.

| | |
|---|---|
| **WICHTIG** | Wenn sich die GuardLogix-Steuerung im Run- oder Programmmodus befindet und Sie das Anwendungsprogramm nicht validiert haben, sind Sie für die Einhaltung der Sicherheitsbedingungen verantwortlich. |

Zudem können die Standard-Tasks in den GuardLogix-Steuerungen entweder für Standardanwendungen oder für Sicherheitsanwendungen nach SIL 2 genutzt werden, wie in Publikation 1756-RM001), „Using ControlLogix in SIL 2 Applications Reference Manual", beschrieben. In beiden Fällen dürfen Sie keine SIL 2- oder Standard-Tasks und -Variablen verwenden, um Sicherheitsregelkreise einer höheren Ebene zu erstellen. Die Sicherheits-Task ist die einzige für SIL 3-Anwendungen zertifizierte Task.

Verwenden Sie die Anwendung Studio 5000 Logix Designer, um Programme für GuardLogix 5570-Steuerungen zu erzeugen.

Der TÜV Rheinland hat GuardLogix-Steuerungssysteme der Serie 5570 für den Einsatz in sicherheitstechnischen Anwendungen bis zu SIL CL 3 zugelassen, bei denen der nicht eingeschaltete Zustand als sicherer Zustand gilt. Alle in diesem Handbuch enthaltenen E/A-spezifischen Beispiele sind darauf ausgerichtet, für typische Systeme zur Gewährleistung der Maschinensicherheit und zur Notfallabschaltung den nicht eingeschalteten Zustand als sicheren Zustand zu erreichen.

**WICHTIG** Als Anwender des Systems sind Sie für Folgendes verantwortlich:

- Konfiguration, SIL-Einstufung und -Validierung aller an das GuardLogix-System angeschlossenen Sensoren und Aktoren
- Projektverwaltung und Durchführung des Funktionstests
- Steuerung des Zugriffs auf das Sicherheitssystem einschließlich Kennwortverwaltung
- Programmierung der Anwendung und Konfiguration der Geräte entsprechend den Informationen in diesem Sicherheitshandbuch und im Benutzerhandbuch „GuardLogix 5570 Controllers User Manual", Publikation 1756-UM022

Beschränken Sie bei der Anwendung der „Funktionalen Sicherheit" den Zugriff auf qualifizierte und autorisierte Mitarbeiter, die über entsprechende Kenntnisse und Erfahrungen verfügen. Die Anwendung Logix Designer umfasst eine kennwortgeschützte Verriegelungsfunktion.

Informationen zur Verwendung dieser Verriegelungsfunktion finden Sie in der Publikation 1756-UM022, „GuardLogix 5570-Steuerungen, Benutzerhandbuch".

## Funktionsprüfungen

Gemäß IEC 61508 müssen Sie die im System verwendeten Geräte verschiedenen Funktionsprüfungen unterziehen. Die Funktionsprüfungen werden zu benutzerdefinierten Zeiten durchgeführt. Beispielsweise können die Funktionsprüfungen einmal im Jahr, einmal alle 15 Jahre oder in einem anderen geeigneten Zeitrahmen durchgeführt werden.

GuardLogix 5570-Steuerungen weisen ein Intervall für die Funktionsprüfung von bis zu 20 Jahren auf. Andere Systemkomponenten wie Sicherheits-E/A-Geräte, Sensoren und Aktoren können über kürzere Intervalle verfügen. Die Steuerung sollte in die Untersuchung der funktionalen Sicherheit der anderen Komponenten im Sicherheitssystem einbezogen werden.

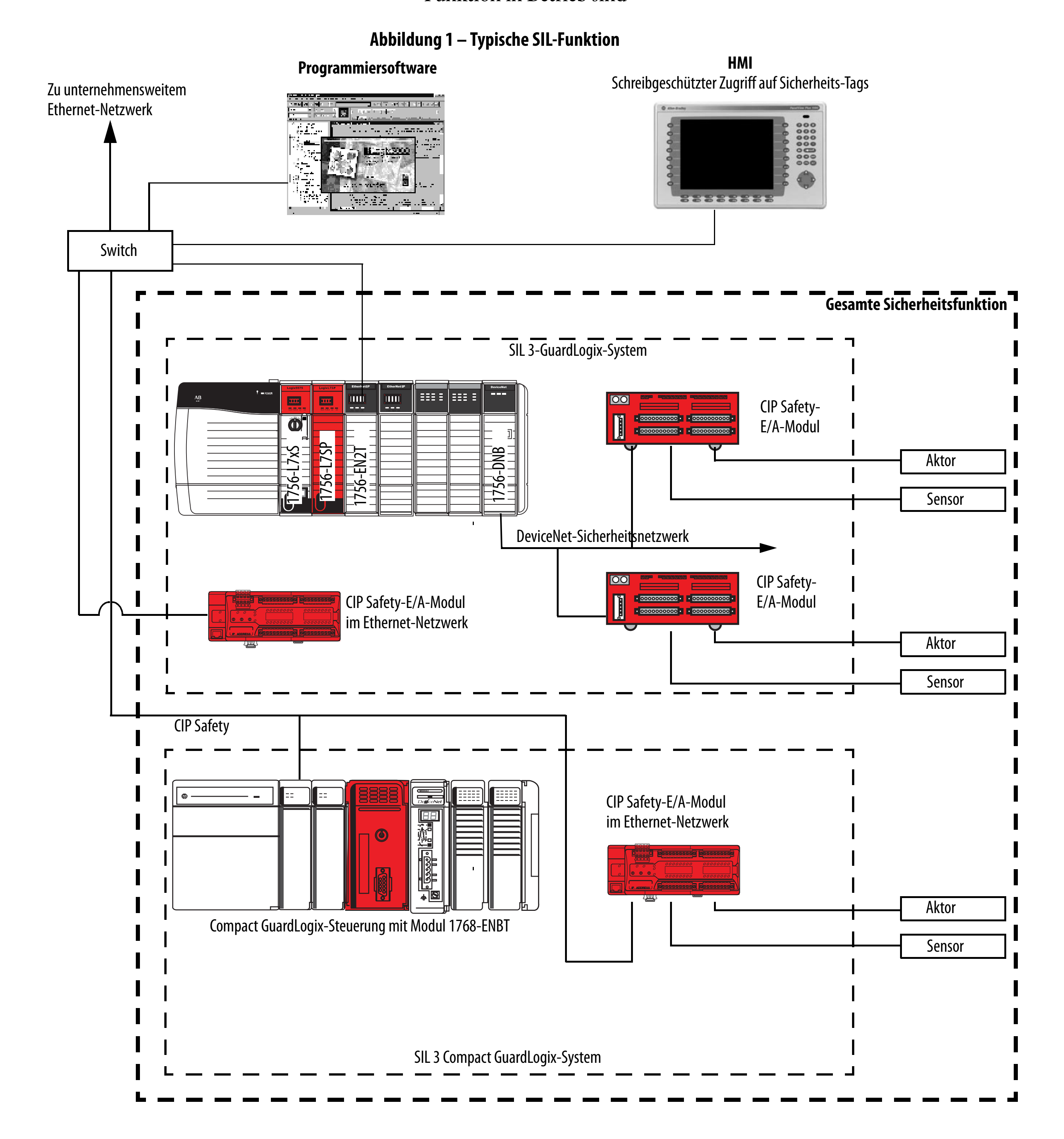
**WICHTIG** Die spezifischen Anwendungen des Anwenders bestimmen das Intervall für die Funktionsprüfung. Dies gilt jedoch in erster Linie für Sicherheits-E/A-Geräte und die Feldinstrumentierung.

## GuardLogix-Architektur für SIL 3-Anwendungen

Die folgende Abbildung zeigt eine typische SIL-Funktion, inklusive der folgenden Punkte:

- Gesamtsicherheitsfunktion
- GuardLogix-Anteil an der Gesamtsicherheitsfunktion
- Anschluss der übrigen Geräte (z. B. HMI), wenn sie außerhalb der Funktion in Betrieb sind

**Abbildung 1 – Typische SIL-Funktion**



## GuardLogix-Systemkomponenten

Die Tabellen in diesem Abschnitt listen die nach SIL 3 zertifizierten GuardLogix-Komponenten sowie die nicht nach SIL 3 zertifizierten Komponenten auf, die mit den SIL 3 GuardLogix-Systemen verwendet werden können.

Eine aktuelle Liste der für GuardLogix-Steuerungen und CIP Safety-E/A-Geräte zertifizierten Produktreihen und Firmware-Versionen finden Sie unter http://www.rockwellautomation.com/products/certification/safety/. Firmware-Versionen sind unter http://support.rockwellautomation.com/ControlFLASH™/ verfügbar.

**Tabelle 2 – SIL 3-zertifizierte GuardLogix-Komponenten**

<table>
<tr><th rowspan="2">Gerätetyp</th><th rowspan="2">Bestell-nummer</th><th rowspan="2">Beschreibung</th><th colspan="2">Verwandte Dokumentationen[3]</th></tr>
<tr><th>Installations-anleitung</th><th>Benutzerhandbuch</th></tr>
<tr><td rowspan="4">1756 GuardLogix Primärsteuerung (ControlLogix5570S)</td><td>1756-L71S</td><td>Steuerung mit 2 MB Standard-, 1 MB Sicherheitsspeicher</td><td rowspan="6">n. v.[4]</td><td rowspan="6">• Mit Studio 5000-Umgebung, ab Version 21: 1756-UM022<br>• Mit der Software RSLogix 5000, bis Version 20: 1756-UM020</td></tr>
<tr><td>1756-L72S</td><td>Steuerung mit 4 MB Standard-, 2 MB Sicherheitsspeicher</td></tr>
<tr><td>1756-L73S</td><td>Steuerung mit 8 MB Standard-, 4 MB Sicherheitsspeicher</td></tr>
<tr><td>1756-L73SXT</td><td>Steuerung (XT) mit 8 MB Standard-, 4 MB Sicherheitsspeicher</td></tr>
<tr><td rowspan="2">1756 GuardLogix Sicherheitspartner (ControlLogix557SP)</td><td>1756-L7SP</td><td>Sicherheitspartner</td></tr>
<tr><td>1756-L7SPXT</td><td>Sicherheitspartner (XT)</td></tr>
<tr><td rowspan="3">1756 GuardLogix Primärsteuerung (ControlLogix5560S)[1]</td><td>1756-L61S</td><td>Steuerung mit 2 MB Standard-, 1 MB Sicherheitsspeicher</td><td rowspan="4">n. v.[4]</td><td rowspan="4">1756-UM020</td></tr>
<tr><td>1756-L62S</td><td>Steuerung mit 4 MB Standard-, 1 MB Sicherheitsspeicher</td></tr>
<tr><td>1756-L63S</td><td>Steuerung mit 8 MB Standard-, 3,75 MB Sicherheitsspeicher</td></tr>
<tr><td>1756 GuardLogix Sicherheitspartner (ControlLogix55SP)[1]</td><td>1756-LSP</td><td>Sicherheitspartner</td></tr>
<tr><td rowspan="2">1768-Compact GuardLogix-Steuerung (CompactLogix4xS)[2]</td><td>1768-L43S</td><td>Steuerung mit Unterstützung für zwei 1768-Module</td><td rowspan="2">n. v.[4]</td><td rowspan="2">1768-UM002</td></tr>
<tr><td>1768-L45S</td><td>Steuerung mit Unterstützung für vier 1768-Module</td></tr>
<tr><td>CIP Safety-E/A-Module in DeviceNet-Netzwerken</td><td colspan="2" rowspan="3">Eine aktuelle Liste der zertifizierten Produktreihen und Firmware-Versionen finden Sie im Sicherheitszertifikat unter http://www.rockwellautomation.com/products/certification/safety/</td><td>1791DS-IN001<br>1791DS-IN002<br>1732DS-IN001</td><td>1791DS-UM001</td></tr>
<tr><td>CIP Safety-E/A-Module in EtherNet/IP-Netzwerken</td><td>1791ES-IN001</td><td>1791ES-UM001</td></tr>
<tr><td>POINT Guard I/O-Module</td><td>n. v.[4]</td><td>1734-UM013</td></tr>
<tr><td>Kinetix 5500-Servoantriebe (Bestellnummern, die mit -ERS2 enden)</td><td colspan="2">Eine aktuelle Liste der zertifizierten Produktreihen und Firmware-Versionen finden Sie im Sicherheitszertifikat unter http://www.rockwellautomation.com/products/certification/safety/</td><td>2198-IN001</td><td>2198-UM001</td></tr>
</table>

(1) Für den Einsatz mit der Software RSLogix 5000, Version 14, Version 16 und höher zertifiziert.

(2) Für den Einsatz mit der Software RSLogix 5000, ab Version 18 zertifiziert.

(3) Diese Publikationen stehen auf der Website von Rockwell Automation unter http://www.rockwellautomation.com/literature zum Abruf bereit.

(4) Installationsanleitung – siehe Benutzerhandbuch.

**Tabelle 3 – Komponenten, die zur Verwendung mit den Sicherheitssystemen der 1756 GuardLogix-Steuerung geeignet sind**

| Gerätetyp | Bestellnummer | Beschreibung | Produkt-reihe(1) | Version(1) | Verwandte Dokumentationen(3) | |
|---|---|---|---|---|---|---|
| | | | | | Installations-anleitung | Benutzer-handbuch |
| Chassis | 1756-A4<br>1756-A7<br>1756-A10<br>1756-A13<br>1756-A17 | Chassis mit 4 Steckplätzen<br>Chassis mit 7 Steckplätzen<br>Chassis mit 10 Steckplätzen<br>Chassis mit 13 Steckplätzen<br>Chassis mit 17 Steckplätzen | B | n. v. | 1756-IN005 | n. v. |
| | 1756-A4LXT<br>1756-A5XT<br>1756-A7XT<br>1756-A7LXT | XT-Chassis mit 4 Steckplätzen<br>XT-Chassis mit 5 Steckplätzen<br>XT-Chassis mit 7 Steckplätzen<br>XT-Chassis mit 7 Steckplätzen | B | n. v. | | |
| Netzteil | 1756-PA72 | AC-Netzteil | C | n. v. | 1756-IN005 | n. v. |
| | 1756-PB72 | DC-Netzteil | C | | | |
| | 1756-PA75 | AC-Netzteil | B | | | |
| | 1756-PB75 | DC-Netzteil | B | | | |
| | 1756-PAXT | XT-Netzteil, AC | B | | | |
| | 1756-PBXT | XT-Netzteil, DC | B | | | |
| Kommunikations-module | 1756-ENBT<br>1756-EN2T<br>1756-EN2F<br>1756-EN2TR<br>1756-EN3TR | EtherNet/IP-Bridge | A<br>A<br>A<br>C<br>B | 3.006<br>2.005<br>2.005<br>10.007<br>10.007 | ENET-IN002 | ENET-UM001 |
| | 1756-EN2TXT<br>1756-EN2TRXT | XT EtherNet/IP-Bridge (Kupfer) | C<br>C | 5.007<br>10.006 | | |
| | 1734-AENT | POINT I/O-Ethernet-Adapter | A | 3.001 | 1734-IN590 | 1734-UM011 |
| | 1756-DNB | DeviceNet-Bridge | A | 6.002 | DNET-IN001 | DNET-UM004 |
| | 1756-CN2 | ControlNet-Bridge | A | 12.001 | CNET-IN005 | CNET-UM001 |
| | 1756-CN2R | ControlNet-Bridge, redundante Medien | A | 12.001 | | |
| | 1756-CN2RXT | XT ControlNet-Bridge, redundante Medien | B | 20.020 | | |
| Programmier-software | 9324-*xxxx* | Software RSLogix 5000 für GuardLogix-Steuerungen 5560 | n. v. | 14(2) | n. v. | Siehe Online-Hilfe. |
| | | Software RSLogix 5000 für GuardLogix-Steuerungen 5570 (XT) | | 20 | | |
| | 9324-*xxxx* | Studio 5000-Umgebung für GuardLogix-Steuerungen 5570 (XT) | | 21 | | |
| Speicherkarten | 1784-CF128 | 128 MB CompactFlash-Karte für GuardLogix 5560-Steuerungen | n. v. | n. v. | n. v. | n. v. |
| | 1784-SD1 | 1 GB Secure Digital (SD)-Karte für GuardLogix-Steuerungen 5570 | | | | |
| | 1784-SD2 | 2 GB Secure Digital (SD)-Karte für GuardLogix-Steuerungen 5570 | | | | |

(1) Diese Version oder höher.
(2) Software RSLogix 5000, Version 15, unterstützt keine GuardLogix-Sicherheitssteuerungen.
(3) Diese Publikationen stehen auf der Website von Rockwell Automation unter http://www.rockwellautomation.com/literature zum Abruf bereit.

Sie können die Steckplätze eines SIL 3-Systemchassis, die nicht vom GuardLogix SIL 3-System verwendet werden, mit anderen ControlLogix-Modulen (1756) belegen, die für die Niederspannungs- und die EMV-Richtlinien zertifiziert sind.

**WICHTIG** Die ControlLogix-XT™-Systemkomponenten sind nur dann für extreme Umgebungsbedingungen ausgelegt, wenn sie ordnungsgemäß mit anderen Logix-XT-Systemkomponenten eingesetzt werden. Die Verwendung von ControlLogix-XT-Komponenten mit herkömmlichen ControlLogix- oder GuardLogix-Systemkomponenten hebt die Auslegung für extreme Umgebungsbedingungen auf.

Zertifikate zur Produktreihe der programmierbaren ControlLogix-Steuerungen finden Sie unter http://www.rockwellautomation.com/products/certification/ce/.

## GuardLogix-Zertifizierungen

In den Technischen Daten zu den ControlLogix-Steuerungen, Publikation 1756-TD001, „ControlLogix Controllers Technical Data“, werden die Produktspezifikationen und die amtlichen Zulassungen aufgeführt, für die die Produkte zugelassen sind. Wenn ein Produkt eine amtliche Zulassung erhalten hat, wird dies auf der Produktetikettierung gekennzeichnet. Die Konformitätserklärung und weitere Einzelheiten zu den Zertifizierungen erhalten Sie, wenn Sie auf den Link „Product Certification“ unter http://www.rockwellautomation.com/products/certification/ klicken.

## GuardLogix-Spezifikationen für PFD und PFH

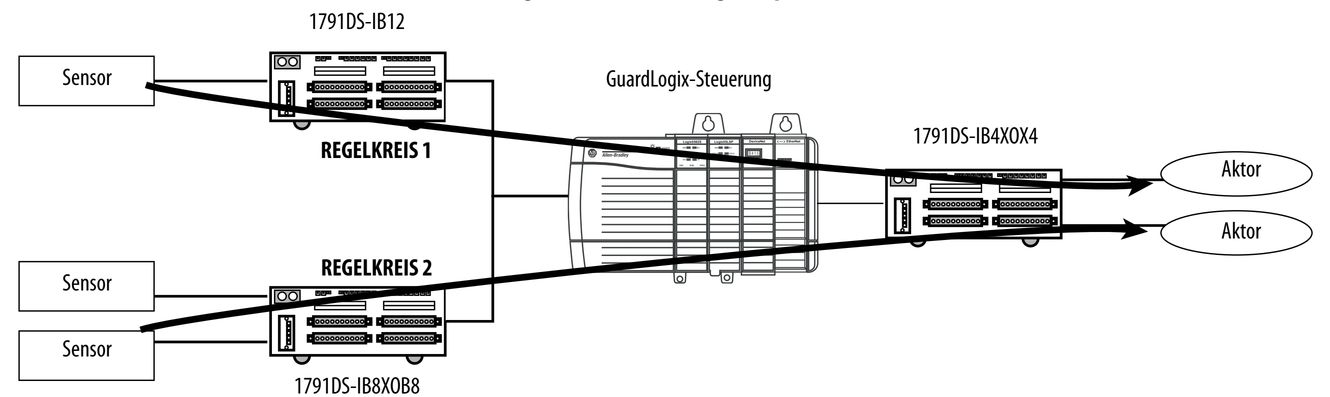
Sicherheitstechnische Systeme können als solche klassifiziert werden, die entweder bei niedriger Beanspruchung oder bei hoher Beanspruchung bzw. im Dauermodus betrieben werden. Die Richtlinie IEC 61508 legt fest, dass das Sicherheitssystem für den Betrieb im Modus für niedrige Beanspruchung mit einer Häufigkeit von nicht mehr als einmal pro Jahr und für den Betrieb im Modus für hohe Beanspruchung bzw. im Dauermodus mehr als einmal pro Jahr angefordert werden darf.

Der SIL-Wert für ein sicherheitstechnisches System für niedrige Beanspruchung hängt direkt mit den Größenordnungsbereichen seiner durchschnittlichen Ausfallwahrscheinlichkeit bei der zufriedenstellenden Durchführung seiner Sicherheitsfunktion oder, einfach, mit der Versagenswahrscheinlichkeit (PFD) zusammen. Der SIL-Wert für ein sicherheitstechnisches System für hohe Beanspruchung hängt direkt mit der Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde (PFH) zusammen.

Die PFD- und PFH-Werte können mit allen drei primären Elementen in Zusammenhang gebracht werden und ergeben zusammen ein sicherheitstechnisches System (die Sensoren, das Logikelement und die Aktoren). Das Logikelement umfasst außerdem Eingangs-, Prozessor- und Ausgangselemente.

Informationen zu den PFD- und PFH-Werten sowie zu den Intervallen der Funktionsprüfung für Guard I/O-Module finden Sie in Anhang E, Sicherheitsdaten der GuardLogix-Systeme.

**Abbildung 2 – PFH-Berechnungsbeispiel**



Um die Logikelement-PFH für jeden Sicherheitsregelkreis in dem oben abgebildeten einfachen Beispiel (PFH-Beispielberechnung) zu berechnen, addieren Sie die PFH-Werte für jede Komponente des Regelkreises. Die Tabelle PFH-Berechnungen nach Sicherheitsregelkreis enthält ein vereinfachtes Beispiel für PFH-Wertberechnungen für jeden Sicherheitsregelkreis in der Abbildung mit dem PFH-Berechnungsbeispiel.

**Tabelle 4 – PFH-Berechnungen nach Sicherheitsregelkreis**

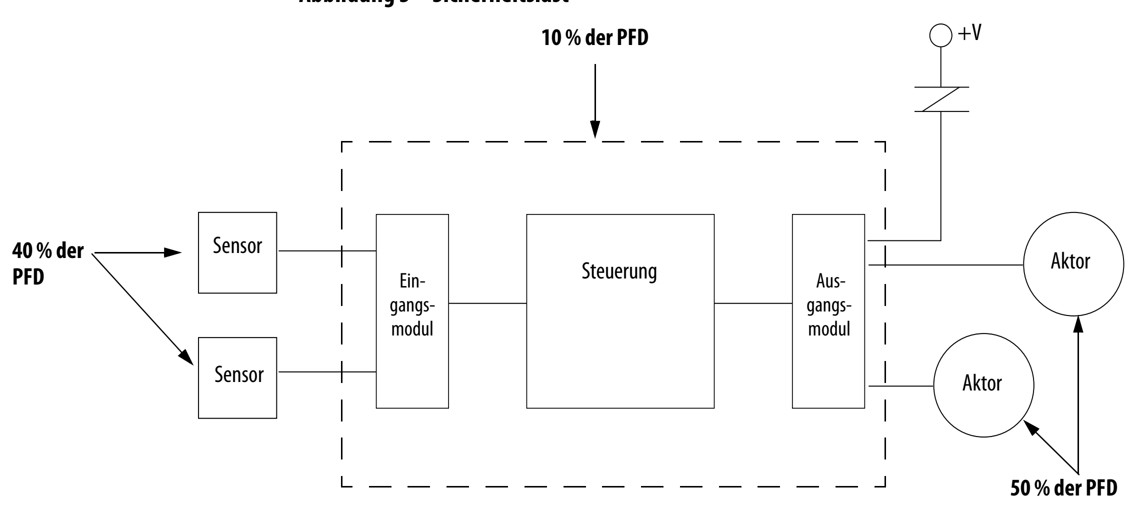
| Für diesen Regelkreis | Die PFH-Werte dieser Komponente addieren |
|---|---|
| Summe PFH für Regelkreis 1 = | 1791DS-IB12 + GuardLogix-Steuerung + 1791DS-IB4XOX4 |
| Summe PFH für Regelkreis 2 = | 1791DS-IB8XOB8 + GuardLogix-Steuerung + 1791DS-IB4XOX4 |

Bei der Berechnung der PFH-Werte sind die spezifischen Anforderungen der eingesetzten Applikation einschließlich Testzeitintervalle zu berücksichtigen.

## SIL-Einhaltung (Safety Integrity Level) – Verteilung und Gewichtung

Nach konservativen Einschätzungen entfällt 10 % der Sicherheitslast auf GuardLogix-Steuerung und -E/A-System. In ein SIL 3-System müssen u. U. mehrere Eingänge für wichtige Sensoren und Eingangsgeräte sowie je nach SIL-Beurteilung des sicherheitstechnischen Systems zwei mit zwei Aktoren in Serie geschaltete Ausgänge integriert werden.

**Abbildung 3 – Sicherheitslast**




## Systemreaktionszeit

Die Systemreaktionszeit ist der Zeitraum zwischen dem Eingang eines sicherheitsrelevanten Ereignisses im System und dem Zeitpunkt, an dem das System die entsprechenden Ausgänge in den sicheren Zustand versetzt. Fehler im System können zudem die Reaktionszeit des Systems beeinträchtigen. Die Systemreaktionszeit ist die Summe der folgenden Reaktionszeiten:




Die einzelnen Reaktionszeiten hängen von unterschiedlichen Faktoren ab, wie dem Typ des E/A-Geräts und den im Programm verwendeten Befehlen.

### Sicherheits-Task-Reaktionszeit

Die Sicherheits-Task-Reaktionszeit ist die längstmögliche Verzögerung einer bei der Steuerung eingehenden Eingangsänderung, bis der verarbeitete Ausgang vom Ausgangs-Producer eingerichtet wird. Dieser Zeitraum ist kleiner als die oder gleich der Summe von Sicherheits-Task-Periode und Sicherheits-Task-Überwachungszeitraum.

### Sicherheits-Task-Periode und Sicherheits-Task-Überwachungs-zeitraum

Die Sicherheits-Task-Periode ist das Intervall, mit dem die Sicherheits-Task ausgeführt wird.

Die Zeit des Sicherheits-Task-Überwachungszeitraums ist die maximal zulässige Zeit für die Verarbeitung der Sicherheits-Task. Wenn die Zeit für die Verarbeitung der Sicherheits-Task über die Zeit des Sicherheits-Task-Überwachungszeitraums hinausgeht, tritt beim Übergang von Steuerung und Ausgang in den sicheren Zustand automatisch ein nicht korrigierbarer Sicherheitsfehler auf.

Die Zeit des Sicherheits-Task-Überwachungszeitraums ist benutzerdefiniert, muss aber kleiner als oder gleich der Sicherheits-Task-Periode sein.

Die Zeit des Sicherheits-Task-Überwachungszeitraums wird in der Anwendung Logix Designer im Fenster für die Task-Eigenschaften eingerichtet. Dieser Wert kann unabhängig vom Steuerungsmodus online geändert werden. Eine Änderung ist jedoch nicht möglich, wenn die Steuerung sicherheitsverriegelt wurde oder wenn eine Sicherheits-Task-Signatur erstellt wurde.

## Ansprechpartner bei Geräteausfall

Wenn Sie eine Störung an einem SIL 3-zertifizierten Gerät feststellen, wenden Sie sich an Ihren Allen-Bradley-Distributor vor Ort, damit folgende Maßnahmen eingeleitet werden können:

- Sie können das Gerät an Rockwell Automation zurücksenden, damit die Störung für die betroffene Bestellnummer entsprechend protokolliert und ein Datensatz für die Störung erstellt wird.
- Sie können eine Störungsanalyse anfordern (falls erforderlich), um zu versuchen, die Ursache der Störung zu ermitteln.

# GuardLogix-Steuerungssystem



Eine kurze Auflistung der Komponenten, die für die Verwendung in SIL 3-Anwendungen (Safety Integrity Level) geeignet sind, finden Sie in der Tabelle auf Seite 16. Aktuelle, ausführliche Informationen finden Sie unter http://www.rockwellautomation.com/products/certification/safety/.

Bei der Installation einer GuardLogix-Steuerung der Serie 5570 sind die Informationen im Benutzerhandbuch „GuardLogix 5570 Controllers User Manual", Publikation 1756-UM022, zu beachten.

## GuardLogix-Steuerung 5570 – Hardware

Die GuardLogix-Steuerung umfasst eine Primärsteuerung (ControlLogix 557*x*S) und einen Sicherheitspartner (ControlLogix 557SP). Diese beiden Module werden in einer 1oo2-Architektur eingesetzt und bilden zusammen eine SIL 3-fähige Steuerung. In den folgenden Abschnitten werden diese Module beschrieben.

Sowohl die Primärsteuerung als auch der Sicherheitspartner führen Funktionstests zur Einschalt- und Laufzeitdiagnose aller sicherheitstechnischen Komponenten der Steuerung durch.

Informationen zum Betrieb der Statusanzeigen finden Sie im Benutzerhandbuch „GuardLogix 5570 Controllers User Manual", Publikation 1756-UM022.

| | |
|---|---|
| **WICHTIG** | Statusanzeigen sind keine zuverlässigen Anzeigen für Sicherheitsfunktionen. Nutzen Sie sie daher nur zur allgemeinen Diagnose während der Inbetriebnahme oder Fehlerbehebung. Statusanzeigen sind daher nicht als Betriebsanzeigen zu verwenden. |

Eine Liste der Bestellnummern für GuardLogix-Sicherheitssteuerungen finden Sie in Tabelle 2 auf Seite 16. Eine Liste der für Sicherheitsanwendungen geeigneten ControlLogix-Standardkomponenten finden Sie in Tabelle 3 auf Seite 17.

### Primärsteuerung

Die Primärsteuerung ist der Prozessor, der Standard- und Sicherheitssteuerungsfunktionen ausführt und mit dem Sicherheitspartner für sicherheitsrelevante Funktionen im GuardLogix-Steuerungssystem kommuniziert. Die Primärsteuerung besteht aus einem zentralen Prozessor, einer E/A-Schnittstelle und einem Speicher.

### Sicherheitspartner

Damit SIL 3-Anforderungen erfüllt werden, muss ein Sicherheitspartner im Steckplatz direkt rechts neben der Primärsteuerung installiert sein. Der Sicherheitspartner ist ein Co-Prozessor, der Redundanz für sicherheitsrelevante Funktionen des Systems bietet.

Die Primärsteuerung konfiguriert den Sicherheitspartner. Das Anwenderprogramm muss nur einmal auf die Primärsteuerung heruntergeladen werden. Die Betriebsart des Sicherheitspartners wird von der Primärsteuerung gesteuert.

### Chassis

Das Chassis stellt die physische Verbindung zwischen Modulen und dem GuardLogix-System 1756 dar. Jeder Ausfall, auch wenn noch so unwahrscheinlich, würde von mindestens einer aktiven Komponente des Systems erkannt. Das Chassis ist damit für die Sicherheitsfrage nicht relevant.

GuardLogix-XT™-Steuerungen müssen ein ControlLogix-XT-Chassis verwenden, um die Einstufung für extreme Umgebungsbedingungen zu erhalten.

### Netzteile

Für den SIL 3-Betrieb der ControlLogix-Netzteile ist keine zusätzliche Konfiguration oder Verdrahtung erforderlich. Jeder Ausfall würde von mindestens einer aktiven Komponente des GuardLogix-Systems erkannt. Das Netzteil ist damit für die Sicherheitsfrage nicht relevant.

GuardLogix-XT-Steuerungen müssen ein ControlLogix-XT-Netzteil verwenden, um die Einstufung für extreme Umgebungsbedingungen zu erhalten.

## Sicherheitsprotokoll CIP Safety

Die sicherheitsrelevante Kommunikation zwischen GuardLogix-Steuerungen findet über produzierte und konsumierte Sicherheits-Tags statt. Diese Sicherheits-Tags basieren auf dem Sicherheitsprotokoll CIP Safety, das auf die Sicherung der Datenintegrität während der Kommunikation ausgerichtet ist.

Weitere Informationen zu Sicherheits-Tags finden Sie in Kapitel 5, Merkmale von Sicherheits-Tags, der Sicherheits-Task und von Sicherheitsprogrammen.

## Sicherheits-E/A-Geräte

Informationen dazu, welche CIP Safety-E/A-Geräte mit GuardLogix-Steuerungen eingesetzt werden können, finden Sie in Kapitel 3.

## Kommunikations-Bridges

Tabelle 5 listet die verfügbaren Kommunikationsschnittstellenmodule auf, die die Kommunikation über EtherNet/IP-, DeviceNet-, und ControlNet-Netzwerke mithilfe des CIP Safety-Protokolls ermöglichen.

**Tabelle 5 – Kommunikationsschnittstellenmodule nach System**

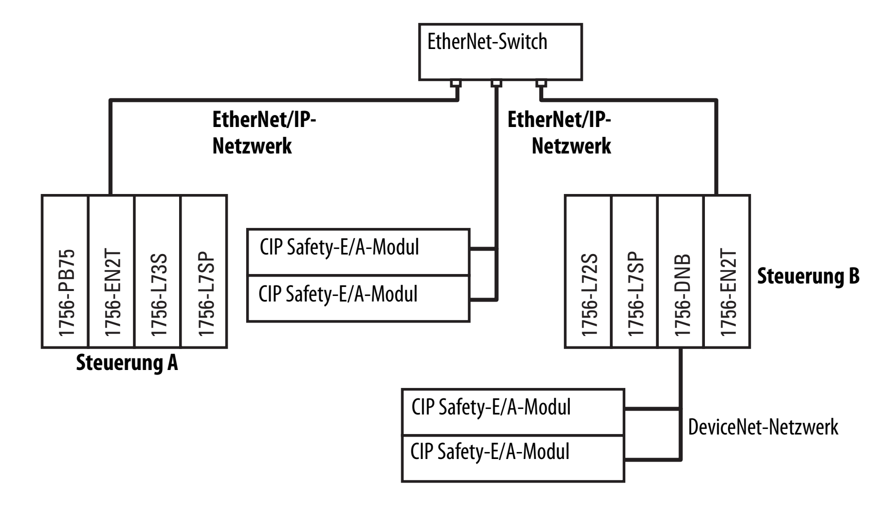
| GuardLogix-System | Kommunikationsmodule |
|---|---|
| 1756 | • 1756-ENBT, 1756-EN2T(R), 1756-EN2F oder 1756-EN3TR, EtherNet/IP-Bridge<br>• 1734-AENT, POINT I/O-Ethernet-Adapter<br>• 1756-DNB, DeviceNet-Bridge<br>• 1756-CN2, ControlNet-Bridge<br>• 1756-CN2R, redundante ControlNet-Bridge |
| 1756 -XT | • 1756-EN2TXT, 1756-EN2TRXT, EtherNet/IP-Bridge – XT (Kupfer)<br>• 1756-CN2RXT, redundante XT-ControlNet-Bridge |
| 1768 | • 1768-ENBT<br>• 1734-AENT, POINT I/O-Ethernet-Adapter<br>• 1768-CNB<br>• 1768-CNBR |

**WICHTIG** Aufgrund des Designs des CIP Safety-Steuerungssystems ist die SIL 3-Zertifizierung für CIP-Sicherheits-Bridges, wie sie in der Tabelle aufgeführt sind, nicht erforderlich.

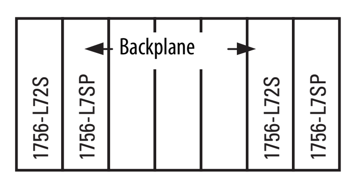
### *EtherNet/IP-Netzwerk*

Die Peer-to-Peer-Sicherheitskommunikation zwischen GuardLogix-Steuerungen ist mithilfe von EtherNet/IP-Bridges über das EtherNet/IP-Netzwerk möglich. Eine EtherNet/IP-Bridge ermöglicht der GuardLogix-Steuerung die Steuerung und den Austausch von Sicherheitsdaten mit CIP Safety-E/A-Geräten in einem EtherNet/IP-Netzwerk.

**Abbildung 4 – Peer-to-Peer-Kommunikation über EtherNet/IP-Bridges und das EtherNet/IP-Netzwerk**



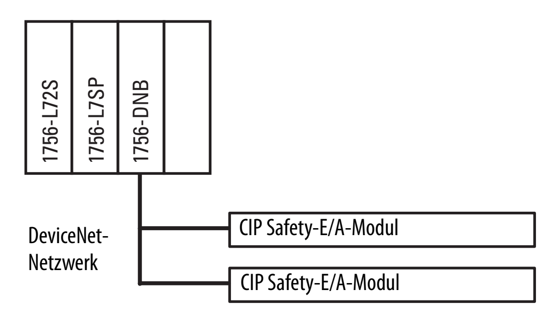
**TIPP** Die Peer-to-Peer-Sicherheitskommunikation zwischen zwei GuardLogix-Steuerungen im selben Chassis ist auch über die Backplane möglich.




*DeviceNet-Sicherheitsnetzwerk*

DeviceNet-Bridges ermöglichen der GuardLogix-Steuerung die Steuerung und den Austausch von Sicherheitsdaten mit CIP Safety-E/A-Modulen in einem DeviceNet-Netzwerk.

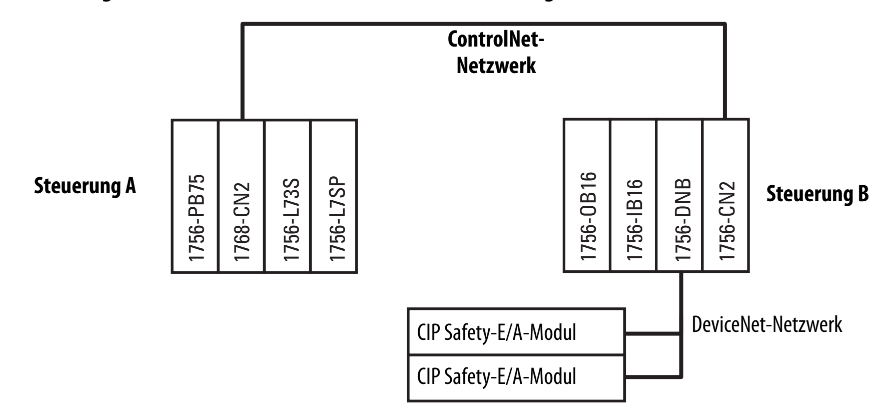
**Abbildung 5 – Kommunikation über eine DeviceNet-Bridge**




*ControlNet-Netzwerk*

ControlNet-Bridges ermöglichen der GuardLogix-Steuerung das Produzieren und Konsumieren von Sicherheits-Tags über ControlNet-Netzwerke zu anderen GuardLogix-Steuerungen oder dezentralen CIP Safety-E/A-Netzwerken.

**Abbildung 6 – Kommunikation über eine ControlNet-Bridge**



## Überblick über die Programmierung

Programmieren Sie GuardLogix 5570-Steuerungen mithilfe der Anwendung Studio 5000 Logix Designer.

Nutzen Sie Logix Designer, um Standort, Verwaltungsrechte und Konfiguration von E/A-Geräten und Steuerungen zu definieren und um die Programmlogik zu erstellen, zu testen und zu entstören. In der GuardLogix-Sicherheits-Task wird nur die Kontaktplanlogik unterstützt.

Informationen zum Befehlssatz für Sicherheitsprojekte finden Sie in Anhang A.

Autorisierte Mitarbeiter können ein Sicherheitsprogramm ändern. Dazu muss jedoch eines der unter Bearbeiten Ihrer Sicherheitsanwendung auf Seite 59 beschriebenen Verfahren verwendet werden.

# Notizen:

# CIP Safety-E/A für das GuardLogix-Steuerungssystem



## Überblick

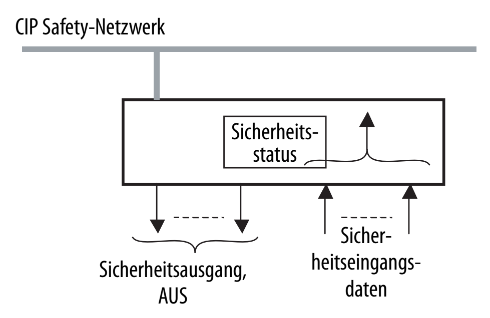
Vor der Inbetriebnahme eines GuardLogix 5570-Sicherheitssystems mit CIP Safety-E/A-Geräten müssen Sie sich mit den Informationen zu Installation, Betrieb und Sicherheit vertraut machen und für die Einhaltung der entsprechenden Anweisungen sorgen. Sie finden diese Informationen in den Publikationen, die in der Tabelle SIL 3-zertifizierte GuardLogix-Komponenten auf Seite 16 aufgelistet sind.

CIP Safety-E/A-Geräte können an Sicherheitseingangs- und -ausgangsgeräte, beispielsweise an Sensoren und Aktoren, angeschlossen werden, sodass sich diese Geräte durch die GuardLogix-Steuerung überwachen und steuern lassen. Bei Sicherheitsdaten erfolgt die E/A-Kommunikation über Sicherheitsverbindungen unter Verwendung des CIP Safety-Protokolls. Die Sicherheitslogik wird in der GuardLogix-Steuerung verarbeitet.

## Typische Sicherheitsfunktionen von CIP Safety-E/A-Geräten

Der folgende Zustand gilt für CIP Safety-E/A-Geräte als sicherer Zustand

- Sicherheitsausgänge: AUS
- Sicherheitseingangsdaten an Steuerung: AUS




Verwenden Sie die CIP Safety-E/A-Geräte für Anwendungen, die sich im sicheren Zustand befinden, nachdem der Sicherheitsausgang ausgeschaltet wurde.

## Diagnose

Die CIP Safety-E/A-Geräte führen beim Einschalten des Stroms sowie in regelmäßigen Abständen während des Betriebs eine Eigendiagnose durch. Wird während der Diagnose ein Fehler festgestellt, dann werden die Sicherheitseingangsdaten (zur Steuerung) und die lokalen Sicherheitsausgänge in ihren sicheren Zustand (AUS) versetzt.

## Statusdaten

Neben den Sicherheitseingangs- und -ausgangsdaten unterstützen CIP Safety-E/A-Geräte Statusdaten zur Überwachung der Geräte und E/A-Schaltkreise. Weitere Informationen zu den spezifischen Funktionen des Produkts entnehmen Sie bitte der Produktdokumentation zu Ihrem Gerät.

## LED-Statusanzeigen

Die CIP Safety-E/A-Geräte sind mit Statusanzeigen versehen. Informationen zum Betrieb dieser Statusanzeigen finden Sie in der Produktdokumentation des von Ihnen eingesetzten Geräts.

## Funktion zur Ein- oder Ausschaltverzögerung

Einige CIP Safety-E/A-Geräte können Funktionen zur Ein- oder Ausschaltverzögerung für Eingangssignale unterstützen. Abhängig von Ihrer Anwendung müssen Sie in die Berechnung der Systemreaktionszeit Ein- und/oder Ausschaltverzögerungen einbeziehen.

Informationen zur Systemreaktionszeit finden Sie in Anhang C.

# Reaktionszeit

Die Eingangsreaktionszeit ist die Zeit ab der Änderung des Signals an einer Eingangsklemme bis zum Zeitpunkt des Versands der Sicherheitsdaten an die GuardLogix-Steuerung.

Die Ausgangsreaktionszeit ist die Zeit ab dem Empfang der Sicherheitsdaten von der GuardLogix-Steuerung bis zum Zeitpunkt der Änderung des Ausgangszustands.

Informationen zur Ermittlung der Eingangs- und Ausgangsreaktionszeiten erhalten Sie in der Produktdokumentation des von Ihnen eingesetzten CIP Safety-E/A-Geräts.

Informationen zur Berechnung der Systemreaktionszeit finden Sie in Anhang C.

## Sicherheitsüberlegungen zu CIP Safety-E/A-Geräten

Sie müssen für alle Geräte, falls erforderlich, eine Netzknoten- oder IP-Adresse und eine Kommunikationsgeschwindigkeit angeben, bevor Sie sie in ein Sicherheitsnetzwerk installieren.

### Verwaltungsrechte

Jedes CIP Safety-E/A-Gerät in einem GuardLogix-System wird nur von einer GuardLogix-Steuerung verwaltet. Bei Bedarf können auch mehrere GuardLogix-Steuerungen und mehrere CIP Safety-E/A-Geräte ohne Einschränkung in Gehäusen oder Netzwerken eingesetzt werden. Wenn eine Steuerung ein E/A-Gerät verwaltet, speichert sie die Konfigurationsdaten des Geräts gemäß Anwenderdefinition. Diese Konfiguration steuert, wie sich die Geräte im System verhalten.

Aus Sicht der Steuerung können Sicherheitsausgangsgeräte nur durch eine einzige Steuerung gesteuert werden. Alle Sicherheitseingangsgeräte werden ebenfalls von einer einzigen Steuerung verwaltet; die Sicherheitseingangsdaten können jedoch von mehreren GuardLogix-Steuerungen gemeinsam genutzt (konsumiert) werden.

### Sicherheits-E/A-Konfigurationssignatur

Die Konfigurationssignatur definiert die Konfiguration des Geräts. Die Signatur kann gelesen und überwacht werden. Die Konfigurationssignatur dient der eindeutigen Definition der Konfiguration eines Geräts. Bei Verwendung einer GuardLogix-Steuerung müssen Sie diese Signatur nicht überwachen. Die GuardLogix-Steuerung überwacht die Signatur automatisch.

### Austausch von E/A-Sicherheitsgeräten

Für den Austausch von Sicherheitsgeräten ist es erforderlich, dass das Ersatzgerät entsprechend konfiguriert wird und dass der Betrieb des Ersatzgeräts durch den Anwender verifiziert wird.

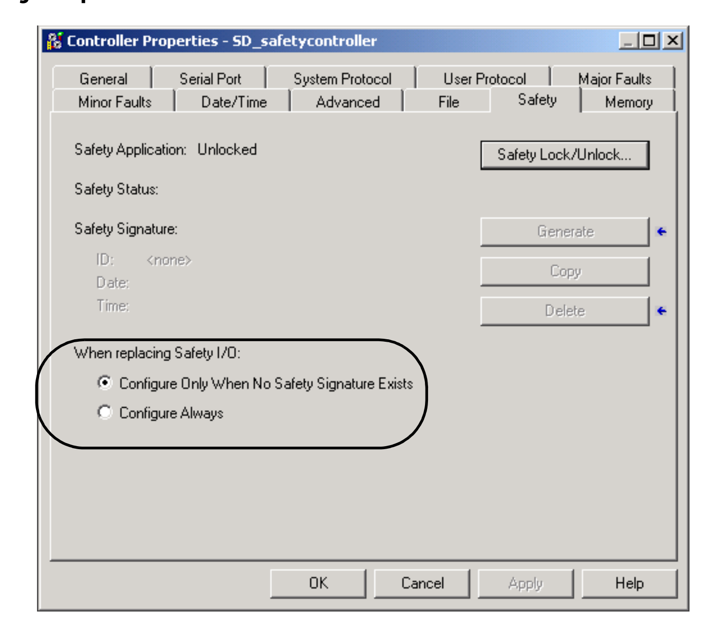


**ACHTUNG:** Während des Austauschs oder eines Funktionstests eines Geräts darf die Sicherheit des Systems in keiner Weise vom betroffenen Gerät abhängen.

In der Anwendung Logix Designer auf der Registerkarte „Safety“ (Sicherheit) im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) gibt es zwei Möglichkeiten, E/A-Geräte auszutauschen:

- Configure Only When No Safety Signature Exists (Nur konfigurieren, wenn keine Sicherheitssignatur vorliegt)
- Configure Always (Immer konfigurieren)

**Abbildung 7 – Optionen für den Austausch von E/A-Sicherheitsmodulen**




### *Configure Only When No Safety Signature Exists (Nur konfigurieren, wenn keine Sicherheitssignatur vorliegt)*

Diese Einstellung weist die GuardLogix-Steuerung an, ein Sicherheitsgerät nur dann zu konfigurieren, wenn die Sicherheits-Task über keine Sicherheits-Task-Signatur verfügt und sich das Austauschgerät im ursprünglichen Zustand befindet, d. h. wenn im Sicherheitsgerät keine Sicherheitsnetzwerknummer vorhanden ist.

Wenn die Sicherheits-Task eine Sicherheits-Task-Signatur hat, konfiguriert die GuardLogix-Steuerung das CIP Safety-E/A-Ersatzgerät nur dann, wenn Folgendes zutrifft:

- Das Gerät verfügt bereits über die korrekte Sicherheitsnetzwerknummer.
- Die elektronische Codierung des Geräts ist korrekt.
- Die Netzknoten- oder IP-Adresse ist korrekt.

*Configure Always (Immer konfigurieren)*

Die GuardLogix-Steuerung versucht stets, ein CIP Safety-E/A-Austauschgerät zu konfigurieren, wenn sich das Gerät im ursprünglichen Zustand befindet, d. h. wenn keine Sicherheitsnetzwerknummer im Sicherheitsaustauschgerät vorliegt und die Netzknotennummer sowie die E/A-Gerät-Codierung mit der Konfiguration der Steuerung übereinstimmen.



**ACHTUNG:** Aktivieren Sie die Funktion „Configure Always“ (Immer konfigurieren) nur, wenn das gesamte Routing-fähige CIP-Safety-Steuerungssystem zur Beibehaltung von SIL 3 während des Austauschs und Funktionstests eines Geräts nicht erforderlich ist.

Wenn andere Bereiche des CIP Safety-Steuerungssystems zur Beibehaltung von SIL 3 erforderlich sind, stellen Sie sicher, dass die Funktion „Configure Always“ der Steuerung deaktiviert ist.

Sie sind dafür verantwortlich, einen Prozess zu implementieren, der sicherstellt, dass die Sicherheitsfunktionalität während des Geräteaustauschs ordnungsgemäß aufrechterhalten bleibt.



**ACHTUNG:** Installieren Sie keine Geräte im Anlieferungszustand in ein CIP Safety-Netzwerk, wenn die Funktion „Configure Always“ aktiviert ist – es sei denn, es wird dabei die in der Publikation 1756-UM022, „GuardLogix 5570-Steuerungen – Benutzerhandbuch“, beschriebene Vorgehensweise eingehalten.

# Notizen:

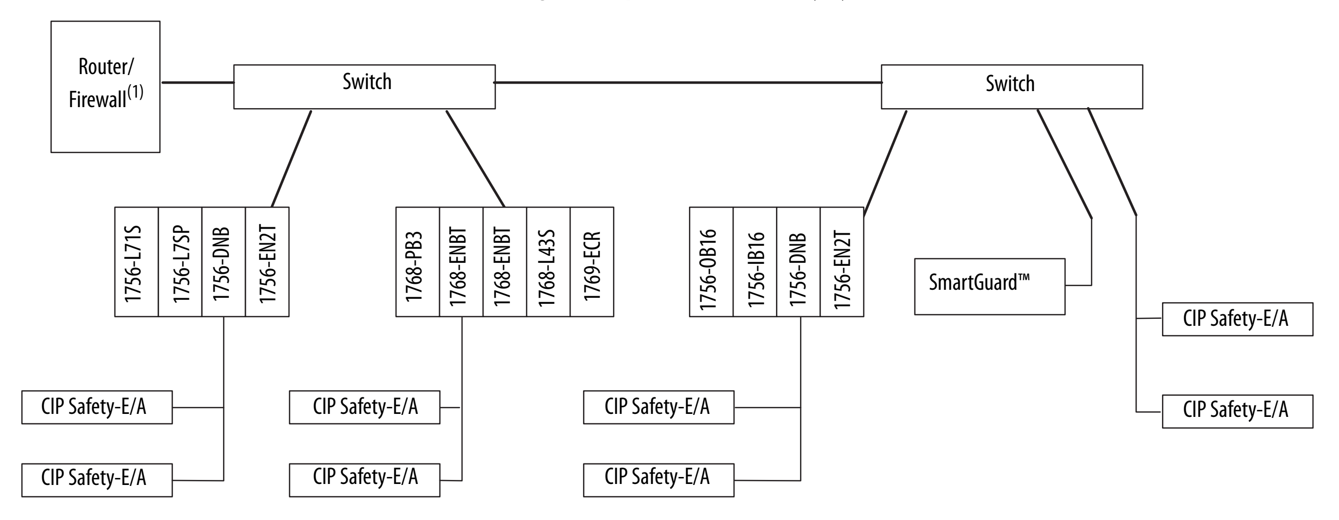
# Informationen zu CIP Safety und zur Sicherheitsnetzwerknummer



## Das Routing-fähige CIP Safety-Steuerungssystem

Um die sicherheitstechnischen Anforderungen eines CIP Safety-Steuerungssystems – einschließlich der Sicherheitsnetzwerknummer (SNN) – zu verstehen, müssen Sie zunächst wissen, wie die Kommunikation in CIP-Steuerungssystemen geroutet werden kann. Das CIP Safety-Steuerungssystem besteht aus einer Reihe von untereinander verbundenen CIP Safety-Geräten. Das Routing-fähige System stellt den Umfang möglicher fehlgeleiteter Pakete vom Originator zu einem Ziel innerhalb des CIP Safety-Steuerungssystems dar. Das System ist isoliert, es bestehen also keine anderen Verbindungen in das System. Da zum Beispiel das in Abbildung 8 abgebildete System nicht mit einem anderen CIP Safety-System über einen größeren (d. h. unternehmensweiten) Ethernet-Backbone verbunden werden kann, stellt es den Umfang eines Routing-fähigen CIP Safety-Systems dar.

**Abbildung 8 – Beispiel für ein CIP Safety-System**




(1) Router oder Firewall werden so konfiguriert, dass sie den Datenverkehr begrenzen.

## Eindeutige Netzknotenreferenz

Das Protokoll „CIP Safety“ stellt ein Endknoten-zu-Endknoten-Sicherheitsprotokoll dar. Dieses Sicherheitsprotokoll ermöglicht das Routing von CIP Safety-Meldungen zu und von CIP Safety-Geräten über nicht zertifizierte Bridges, Switches und Router.

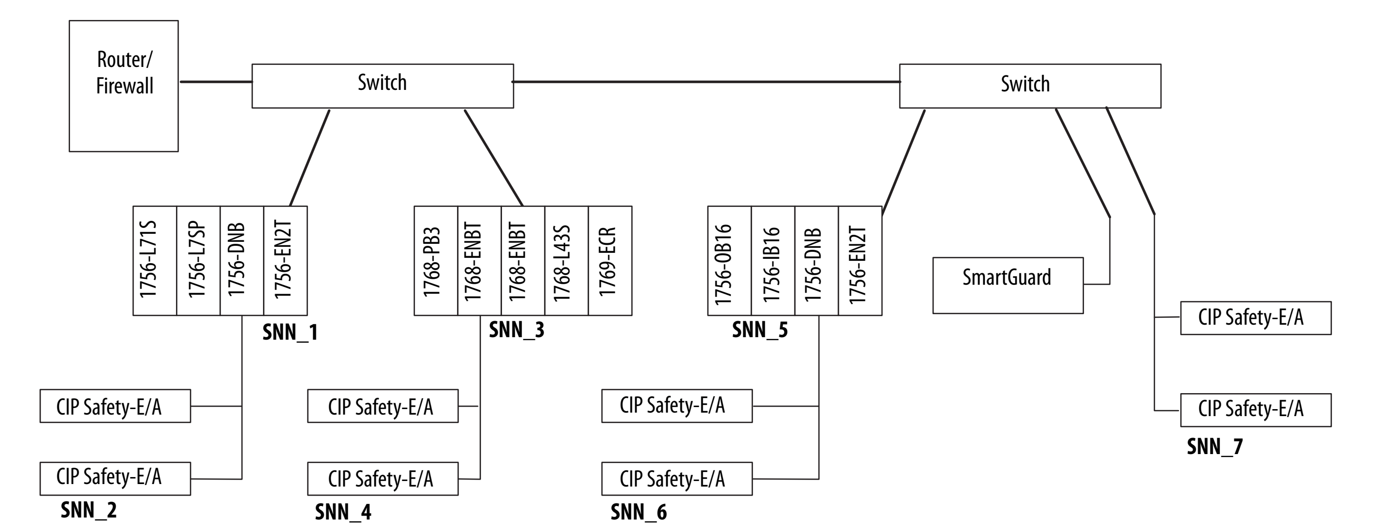
Um zu verhindern, dass Fehler bei nicht zertifizierten Bridges, Switches oder Routern gefährliche Bedingungen verursachen, muss jeder Endknoten mit einem Routing-fähigen CIP Safety-Steuerungssystem über eine eindeutige Netzknotenreferenz verfügen. Die eindeutige Netzknotenreferenz ist eine Kombination aus der Sicherheitsnetzwerknummer (SNN) und der Netzknotenadresse des Netzknotens.

## Sicherheitsnetzwerknummer

Die Sicherheitsnetzwerknummer (SNN) wird automatisch durch die Software oder manuell durch Sie zugeordnet. Jedes CIP Safety-Netzwerk, das Sicherheits-E/A-Knoten enthält, muss über mindestens eine eindeutige SNN verfügen. Jedes Chassis, das mindestens ein Sicherheitsgerät enthält, muss über mindestens eine eindeutige SNN verfügen. Sicherheitsnetzwerknummern, die einem Sicherheitsnetzwerk oder Netzwerk-Subnetz zugeordnet sind, müssen eindeutig sein.

**TIPP** Mehrere SNNs können einem CIP Safety-Subnetz oder Chassis zugeordnet werden, das mehrere Sicherheitsgeräte enthält. Der Einfachheit halber wird jedoch empfohlen, jedem CIP Safety-Subnetz nur eine einzige, eindeutige SNN zuzuordnen. Diese Empfehlung gilt auch für die jeweiligen Chassis.

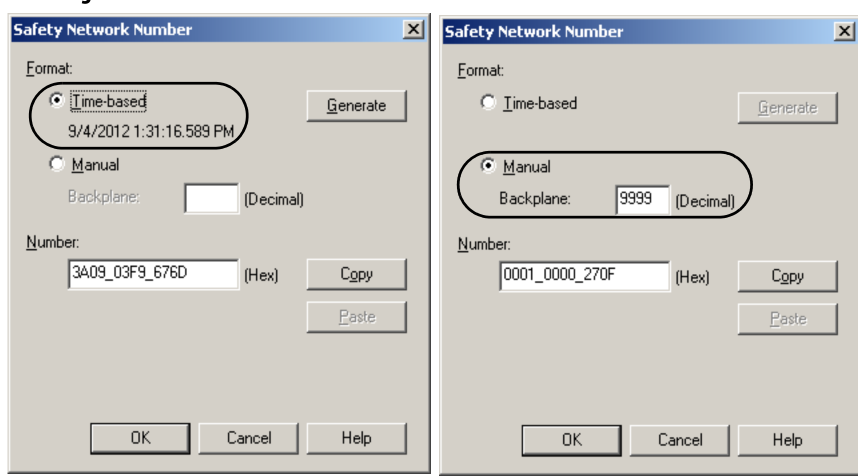
**Abbildung 9 – Beispiel für CIP Safety mit mehreren SNN**




Jedes CIP Safety-Gerät muss mit einer SNN konfiguriert werden. Jedes Gerät, von dem eine Sicherheitsverbindung zu einem anderen Sicherheitsgerät ausgeht, muss mit der SNN des Zielgeräts konfiguriert werden. Wenn sich das CIP Safety-System vor der Prüfung der funktionalen Sicherheit des Systems im Inbetriebnahmevorgang befindet, kann das Ausgangsgerät dazu verwendet werden, die eindeutige Netzknotenreferenz im Gerät einzurichten.

Die vom System verwendete SNN ist eine hexadezimale Zahl mit sechs Byte. Die SNN kann in einem von zwei Formaten eingerichtet und angezeigt werden: zeitbasiert oder manuell. Wenn das zeitbasierte Format ausgewählt wird, beinhaltet die SNN eine lokalisierte Datums- und Uhrzeitangabe. Wenn das manuelle Format ausgewählt ist, beinhaltet die SNN einen Netzwerktyp und einen Dezimalwert von 1 bis 9999.

**Abbildung 10 – SNN-Formate**




Die Zuordnung einer zeitbasierten SNN erfolgt automatisch, wenn Sie ein GuardLogix-Sicherheitssteuerungsprojekt erstellen und neue CIP Safety-E/A-Geräte hinzufügen.

Eine manuelle Manipulation der SNNs ist in den folgenden Situationen erforderlich:

- Wenn konsumierte Sicherheits-Tags verwendet werden.
- Wenn das Projekt Sicherheitseingangsdaten von einem Gerät konsumiert, dessen Konfiguration von einem anderen Sicherheitsgerät verwaltet wird.
- Wenn ein Sicherheitsprojekt in eine andere Hardwareinstallation innerhalb desselben Routing-fähigen CIP Safety-Systems kopiert wird.

| | |
|---|---|
| **WICHTIG** | Wenn Sie SNNs manuell zuordnen, vergewissern Sie sich, dass die Systemerweiterung nicht zu einer Verdoppelung der Kombinationen aus SNN und Netzknotenadresse führt. Ein Verifizierungsfehler tritt auf, wenn Ihr Projekt eine Kombination aus doppelter SNN und Netzknotenadresse umfasst. |

## Hinweise zur Zuordnung der SNN

Die Zuordnung der SNN hängt von Faktoren ab, wie z. B. der Konfiguration der Steuerung oder des CIP Safety-E/A-Geräts.

### SNN für konsumierte Sicherheits-Tags

Wenn eine Sicherheitssteuerung mit produzierten Sicherheits-Tags der E/A-Konfigurationsstruktur hinzugefügt wird, muss die SNN der produzierenden Steuerung eingegeben werden. Die SNN kann aus dem Projekt der produzierenden Steuerung kopiert und in die neue Steuerung eingefügt werden, die der E/A-Konfigurationsstruktur hinzugefügt wird.

Informationen zum Kopieren und Einfügen einer SNN finden Sie in der Publikation 1756-UM022, „GuardLogix 5570-Steuerungen – Benutzerhandbuch“.

## Sicherheitsnetzwerknummer (SNN) für Geräte im Anlieferungszustand

CIP Safety-E/A-Geräte weisen im Anlieferungszustand keine SNN auf. Die SNN wird festgelegt, wenn eine Konfiguration von der GuardLogix-Steuerung, die Verwaltungsrechte für das Gerät besitzt, an das Gerät gesendet wird.

| | |
|---|---|
| **WICHTIG** | Damit ein CIP Safety-E/A-Gerät zu einem konfigurierten GuardLogix-System hinzugefügt werden kann (die SNN ist in der GuardLogix-Steuerung vorhanden), muss das CIP Safety-E/A-Austauschgerät die richtige SNN anwenden, bevor es dem CIP Safety-Netzwerk hinzugefügt wird. |

## SNN für Sicherheitsgeräte mit verschiedenen Konfigurationsverwaltern

Wenn ein CIP Safety-E/A-Gerät von einer anderen GuardLogix-Steuerung (Steuerung B) verwaltet und dann zu einem anderen GuardLogix-Projekt (Projekt Steuerung A) hinzugefügt wird, ordnet die Anwendung Logix Designer automatisch eine SNN basierend auf dem aktuellen Projekt zu. Da das aktuelle Projekt (Projekt Steuerung A) nicht der tatsächliche Konfigurationsverwalter ist, muss die ursprüngliche SNN (Projekt Steuerung B) in die Konfiguration des Projekts der Steuerung A kopiert werden. Dies wird mithilfe der Standardbefehle zum Kopieren und Einfügen einfach bewerkstelligt. Dies führt dazu, dass das CIP Safety-E/A-Gerät Daten gleichzeitig für zwei GuardLogix-Steuerungen produziert. Das Kopieren und Einfügen ist für maximal 16 Steuerungen zulässig.

Informationen zum Ändern, Kopieren und Einfügen von Sicherheitsnetzwerknummern finden Sie in der Publikation 1756-UM022, „GuardLogix 5570-Steuerungen – Benutzerhandbuch“.

## SNN beim Kopieren eines Sicherheitsprojekts



**ACHTUNG:** Wird ein Sicherheitsprojekt in ein anderes Projekt kopiert, das auf eine andere Hardwareinstallation ausgerichtet ist oder sich an einem anderen physischen Standort befindet und bei dem die Installation innerhalb desselben Routing-fähigen CIP Safety-Systems bleibt, muss jede SNN im zweiten System geändert werden. SNN-Werte dürfen sich nicht wiederholen.

Informationen zum Ändern der SNN finden Sie in der Publikation 1756-UM022, „GuardLogix 5570-Steuerungen – Benutzerhandbuch“.

# Merkmale von Sicherheits-Tags, der Sicherheits-Task und von Sicherheitsprogrammen



## Unterscheidung zwischen Standard und Sicherheit

Da es sich um eine Steuerung der Logix-Serie handelt, können im GuardLogix-Steuerungssystem sowohl standardmäßige (d. h. nicht sicherheitstechnische) als auch sicherheitstechnische Komponenten verwendet werden.

Anhand der Standard-Tasks in einem GuardLogix-Projekt können Sie eine standardmäßige Automatisierungssteuerung realisieren. Die GuardLogix-Steuerungen bieten dieselbe Funktionalität wie andere Steuerungen der Serie ControlLogix. Die Steuerungen der GuardLogix-Serie unterscheiden sich von Standardsteuerungen dahingehend, dass sie eine SIL 3-fähige Sicherheits-Task bieten.

Sie müssen jedoch logisch und physisch zwischen den Standard- und Sicherheitsteilen der Anwendung unterscheiden. Die Anwendung Logix Designer ermöglicht diese Unterscheidung über die Sicherheits-Task, Sicherheitsprogramme, Sicherheitsroutinen, Sicherheits-Tags und Sicherheits-E/A-Geräte. Mit der Sicherheits-Task der GuardLogix-Steuerung können Sie eine Sicherheitssteuerung der Stufen SIL 2 und SIL 3 implementieren.

# Sicherheitsanwendungen nach SIL 2

Sie können eine Sicherheitssteuerung nach SIL 2 implementieren, indem Sie die Sicherheits-Task der GuardLogix-Steuerung verwenden.

Da die GuardLogix-Steuerungen zu den Prozessoren der ControlLogix-Serie gehören, können Sie mit einer GuardLogix-Steuerung eine Sicherheitssteuerung nach SIL 2 implementieren. Dies geschieht einfach über die Standard-Tasks oder die Sicherheits-Task. Diese Funktionalität bietet einzigartige und vielseitige Optionen für eine Sicherheitssteuerung, da die meisten Anwendungen prozentual über mehr SIL 2- als SIL 3-Sicherheitsfunktionen verfügen.

## Sicherheitssteuerung nach SIL 2 in der Sicherheits-Task

Die GuardLogix-Sicherheits-Task kann dazu verwendet werden, sowohl SIL 2- als auch SIL 3-Sicherheitsfunktionen bereitzustellen. Sollen SIL 3- und SIL 2-Sicherheitsfunktionen gleichzeitig ausgeführt werden, müssen Sie dafür sorgen, dass nicht nur die in diesem Kapitel unter SIL 3-Sicherheit – die Sicherheits-Task, Sicherheitsprogramme und Sicherheitsroutinen beschriebenen Voraussetzungen sondern auch die in diesem Abschnitt aufgeführten Voraussetzungen für SIL 2 erfüllt sind.

### *SIL 2-Sicherheitslogik*

Aus der Perspektive einer GuardLogix-Sicherheitssteuerung besteht der größte Unterschied zwischen Sicherheitsgeräten nach SIL 2 und SIL 3 darin, dass es sich bei SIL 2 im Allgemeinen um nur einkanalige, bei SIL 3 dagegen in der Regel um zweikanalige Geräte handelt. Wenn Sie sicherheitstechnische Guard I/O-Module (rote Module) einsetzen, die in der Sicherheits-Task erforderlich sind, dann kann es sich bei den Sicherheitseingängen nach SIL 2 um einkanalige Eingänge handeln, wodurch sich sowohl die Komplexität des Systems als auch die Zahl der benötigten Module verringert.

Der Entwickler des Sicherheitssystems ist dafür verantwortlich, alle Sicherheitsfunktionen ordnungsgemäß zu implementieren. Dabei ist Folgendes zu beachten:

- Auswahl der Feldgeräte (korrekte Auswahl, Identifizierung und Behebung von allen Gerätefehlern)
- Berücksichtigung der Sicherheitsanforderungen (gering IEC 61511 oder hoch ISO 13849)
- Berücksichtigung von Testintervallen (Diagnose und Prüfungen, die erforderlich sind, um die Anforderungen der Anwendung zu erfüllen)
- Identifizierung aller verwendeten Fehlerausschlüsse und Begründung anhand der ordnungsgemäßen Dokumentation

| | |
|---|---|
| **WICHTIG** | Werden in der Sicherheits-Task gleichzeitig SIL 2- und SIL 3-Sicherheitsfunktionen verwendet (Kombination), dann müssen Sie verhindern, dass die SIL 2-Eingangssignale direkt die SIL 3-Sicherheitsfunktionen steuern. Verwenden Sie spezifische Sicherheits-Task-Programme oder -Routinen, um SIL 2- und SIL 3-Funktionen voneinander zu trennen. |

Die Anwendung Logix Designer enthält in der Sicherheits-Task eine Reihe von sicherheitstechnischen Kontaktplanbefehlen. GuardLogix-Steuerungen stellen auch anwendungsspezifische Sicherheitsbefehle mit SIL 3-Klassifizierung zur Verfügung. All diese Logikbefehle können in Sicherheitsfunktionen der Kategorie 1 bis 4 und SIL 1 bis 3 verwendet werden.

Soll nur die Sicherheitsstufe SIL 2 erreicht werden, ist keine Sicherheits-Task-Signatur erforderlich. Sobald jedoch SIL 3-Sicherheitsfunktionen in der Sicherheits-Task verwendet werden, ist eine Sicherheits-Task-Signatur erforderlich.

Für SIL 2-Anwendungen empfiehlt es sich, die Sicherheits-Task nach Abschluss der Tests mit einer Sicherheitsverriegelung zu schützen. Durch das Verriegeln der Sicherheits-Task werden weitere Sicherheitsfunktionen aktiviert. Außerdem können Sie den von FactoryTalk® Security und Logix Designer gebotenen Quellenschutz für Routinen verwenden, um den Zugriff auf die sicherheitstechnische Logik zu beschränken.

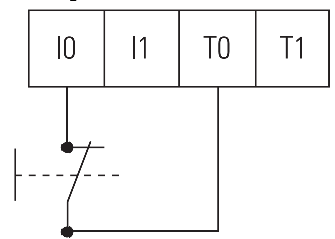
Informationen zur Erzeugung einer Sicherheits-Task-Signatur und zur Verriegelung der Sicherheits-Task finden Sie in der Publikation 1756-UM022, „GuardLogix 5570-Steuerungen – Benutzerhandbuch".

### *SIL 2-Sicherheitseingänge*

Die Sicherheitseingangsmodule CompactBlock™ Guard I/O (Serie 1791), ArmorBlock® Guard I/O (Serie 1732) und POINT Guard I/O (Serie 1734) unterstützen einkanalige SIL 2-Sicherheitseingangsschaltungen. Da diese Module auch auf den SIL 3-Betrieb ausgelegt sind, ist eine Kombination aus SIL 2- und SIL 3-Schaltungen auf demselben Modul zulässig – vorausgesetzt, Sie halten die folgenden Leitlinien ein.

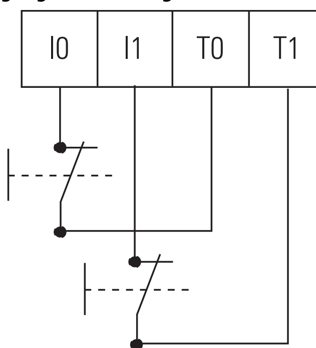
Die nachfolgenden beiden Verdrahtungsbeispiele zeigen, wie SIL 2-Sicherheitsschaltungen mit Guard I/O-Sicherheitseingangsmodulen verdrahtet werden. In diesen Beispielen kommen die integrierten Testquellen (T0…T*x*) zum Einsatz, die sich auf allen Sicherheitseingangsmodulen der Serien 1791 und 1732 befinden.

**Abbildung 11 – Eingangsverdrahtung**



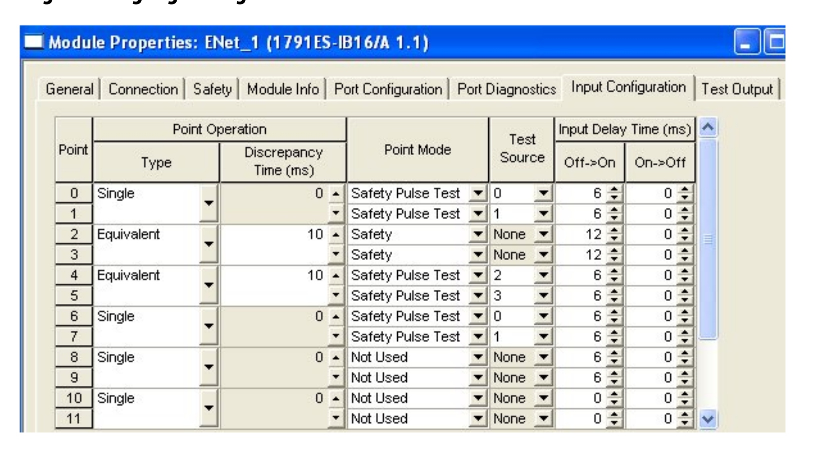

Auf den Guard I/O-Modulen sind die Eingänge paarweise zusammengefasst, um Sicherheitsfunktionen nach Kategorie 3, Kategorie 4 und SIL 3 zu vereinfachen. Bei der Verwendung in Sicherheitsfunktionen nach Kategorie 1, Kategorie 2 und SIL 2 sollten die Moduleingänge weiterhin – wie abgebildet – paarweise verwendet werden. Die Abbildung zeigt zwei SIL 2-Sicherheitsfunktionen, die mit den Eingängen I0 und I1 verdrahtet sind und die Testquellen T0 bzw. T1 verwenden.

**Abbildung 12 – Paarweise Eingangsverdrahtung**




Für Sicherheitsfunktionen nach Kategorie 1, Kategorie 2 und SIL 2 benötigen die Guard I/O-Sicherheitsmodule eine spezifische Konfiguration im GuardLogix-Projekt. In diesem Beispiel sind die Eingänge 0, 1, 6, 7, 8, 9, 10 und 11 Teil einer Sicherheitsfunktion nach Kategorie 1, 2 oder SIL 2. Die Eingänge 2 und 3 sowie die Eingänge 4 und 5 sind Teil einer Sicherheitsfunktion nach Kategorie 3, Kategorie 4 oder SIL 3.

**Abbildung 13 – Eingangskonfiguration**




| Feld | Wert |
|---|---|
| Typ | Single |
| Discrepancy Time | n. v. |
| Point Mode | Safety Pulse Test |
| Test Source | Das Festlegen dieser Werte basiert darauf, wie das Feldgerät physisch mit dem Modul verdrahtet ist. Rufen Sie die Registerkarte „Test Output“ auf und überprüfen Sie die Einstellungen auf dieser Registerkarte, um sicherzustellen, dass die Testquelle korrekt aktiviert wurde. |
| Input Delay Time | Benutzereingabe basierend auf den Leistungsmerkmalen des Feldgeräts. |

**WICHTIG** Die integrierten Impulstestausgänge (T0 bis Tx) werden typischerweise mit Feldgeräten verwendet, die über mechanische Kontakte verfügen. Wenn ein Sicherheitsgerät verwendet wird, das über elektronische Ausgänge verfügt (zur Speisung von Sicherheitseingängen), müssen diese für die entsprechende Sicherheitskategorie ausgelegt sein.

| | |
|---|---|
| **WICHTIG** | Wenn Sie Befehle von GuardLogix-Sicherheitsanwendungen verwenden, müssen Sie sicherstellen, dass Sie Ihre Sicherheitseingangsmodule als „Single" und nicht als „Equivalent" oder „Complementary" konfigurieren. Diese Befehle stellen die gesamte Zweikanal-Funktionalität zur Verfügung, die für PLd- (Cat. 3) oder PLe- (Cat. 4) Sicherheitsfunktionen erforderlich sind.<br>Lesen Sie dazu das Referenzhandbuch „Befehlssatz für GuardLogix-Sicherheitsanwendungen", Publikation 1756-RM095. |

### SIL 2-Sicherheitssteuerung in Standard-Tasks

Aufgrund der Qualität und des Umfangs der Diagnose, die in die ControlLogix-Steuerungen integriert ist, können Sie SIL 2-Sicherheitsfunktionen aus Standard-Tasks heraus ausführen. Dies gilt auch für Steuerungen der Serie GuardLogix.

Um eine SIL 2-Sicherheitssteuerung mit einer GuardLogix-Standard-Task zu realisieren, müssen Sie die Anforderungen erfüllen, die im Referenzhandbuch „Using ControlLogix in SIL 2 Applications Reference Manual", Publikation 1756-RM001, definiert sind.

## SIL 3-Sicherheit – die Sicherheits-Task

Bei Erstellung eines GuardLogix-Projekts wird automatisch eine einzelne Sicherheits-Task erstellt. Die Sicherheits-Task zeichnet sich durch die folgenden zusätzlichen Merkmale aus:

- GuardLogix-Steuerungen sind die einzigen Steuerungen, die die Sicherheits-Task unterstützen.
- Die Sicherheits-Task kann nicht gelöscht werden.
- GuardLogix-Steuerungen unterstützen eine einzelne Sicherheits-Task.
- Innerhalb der Sicherheits-Task können Sie mehrere aus diversen Sicherheitsroutinen bestehende Sicherheitsprogramme verwenden.
- Sie können Standardroutinen nicht aus der Sicherheits-Task heraus planen oder ausführen.

Die Sicherheits-Task ist eine periodische/zeitgesteuerte Task mit einer Task-Priorität und einem Überwachungszeitraum, die vom Anwender ausgewählt werden können. Ihr sollte in der Regel die höchste Priorität der Steuerung zugewiesen werden und der benutzerdefinierte Programmüberwachungszeitraum muss so eingestellt sein, dass Schwankungen in der Ausführung der Sicherheits-Task berücksichtigt werden.

## Einschränkungen der Sicherheits-Task

Sie legen sowohl die Sicherheits-Task-Periode als auch den Sicherheits-Task-Überwachungszeitraum fest. Bei der Sicherheits-Task-Periode handelt es sich um die Periode, mit der die Sicherheits-Task ausgeführt wird. Der Sicherheits-Task-Überwachungszeitraum umfasst die maximale Zeit, die vom Start der für die Sicherheits-Task geplanten Ausführung bis zu ihrem Abschluss erlaubt ist.

Weitere Informationen zum Sicherheits-Task-Überwachungszeitraum finden Sie in Anhang C, Reaktionszeiten.

Die Sicherheits-Task-Periode ist auf maximal 500 ms begrenzt und kann nicht online geändert werden. Stellen Sie sicher, dass der Sicherheits-Task genügend Zeit zum Abschluss bleibt, bevor sie erneut ausgelöst wird. Ein Timeout des Sicherheits-Task-Überwachungszeitraums, ein nicht korrigierbarer Sicherheitsfehler in der GuardLogix-Steuerung, tritt auf, wenn die Sicherheits-Task ausgelöst wird, während sie noch ausgelöst vom vorherigen Trigger ausgeführt wird.

Weitere Informationen finden Sie in Kapitel 7, Überwachung des Status und Handhabung von Störungen.

## Ausführung der Sicherheits-Task

Die Sicherheits-Task wird auf die gleiche Weise wie periodische Standardaufgaben ausgeführt, allerdings mit den folgenden Ausnahmen:

- Die Ausführung der Sicherheits-Task beginnt erst, wenn die Primärsteuerung und der Sicherheitspartner ihre Steuerungspartnerschaft festgelegt haben und die koordinierte Systemzeit (CST) synchronisiert ist. Die Ausführung von Standardaufgaben beginnt jedoch, sobald die Steuerung in den RUN-Modus übergeht.

- Der konfigurierbare Bereich des angeforderten Paketintervalls (RPI) für Sicherheitseingänge und konsumierte Sicherheits-Tags liegt zwar zwischen 6 und 500 ms, doch Sicherheitseingangs-Tags und konsumierte Sicherheits-Tags werden nur zu Beginn der Ausführung der Sicherheits-Task aktualisiert. Dies bedeutet, dass sich die Daten während der Ausführung der Sicherheits-Task auch dann nicht ändern, wenn das angeforderte Paketintervall der E/A kürzer ist als der Zeitraum der Sicherheits-Task. Die Daten sind nur einmal, zu Beginn der Ausführung der Sicherheits-Task schreibgeschützt.

- Sicherheitseingangswerte werden beim Start der Ausführung der Sicherheits-Task „eingefroren". Daher haben timerbezogene Befehle (z. B. TON, TOF usw.) keinen Einfluss auf die Zeit, die während einer Ausführung einer Sicherheits-Task abläuft. Sie messen genau die Zeit von einer Task-Ausführung zur anderen, wobei sich die Zeitbasis während der Ausführung der Sicherheits-Task nicht ändert.



**ACHTUNG:** Dieses Verhalten unterscheidet sich von der Ausführung von Logix-Standard-Tasks, ähnelt jedoch dem Verhalten von SPS oder SLC™.

- Bei Standard-Tags, die Sicherheits-Tags zugewiesen sind, werden die Standard-Tag-Werte beim Start der Sicherheits-Task in den Sicherheitsspeicher kopiert und bleiben während der Ausführung der Sicherheits-Task unverändert.

- Die Werte des Sicherheitsausgangs-Tags (ausgegeben und produziert) werden aktualisiert, sobald die Ausführung der Sicherheits-Task endet.

- Die Sicherheits-Task reagiert auf Modusänderungen (d. h. Ausführung zu Programm oder Programm zu Ausführung) in zeitgesteuerten Intervallen. Daher kann die Sicherheits-Task mehr als eine Task-Periode benötigen, aber immer weniger als zwei, um einen Modusübergang zu vollziehen.

| | |
|---|---|
| **WICHTIG** | Während die Steuerung sicherheitsentriegelt ist und keine Sicherheits-Task-Signatur besitzt, verhindert sie den gleichzeitigen Schreibzugriff auf den Sicherheitsspeicher durch die Sicherheits-Task und die Kommunikationsbefehle. Daher kann die Sicherheits-Task verzögert werden, bis ein Kommunikationsupdate abgeschlossen ist. Die für das Update benötigte Zeit hängt von der Tag-Größe ab. Daher könnten Timeouts der Sicherheitsverbindung und des Sicherheitsüberwachungszeitraums auftreten. (Wenn Sie zum Beispiel Online-Bearbeitungen bei auf 1 ms eingestellter Geschwindigkeit der Sicherheits-Task vornehmen, könnte ein Timeout des Sicherheitsüberwachungszeitraums auftreten.)<br>Zum Ausgleich der Verzögerungszeit aufgrund eines Kommunikationsupdates sollten dem Sicherheitsüberwachungszeitraum 2 ms hinzugefügt werden.<br>Wenn die Steuerung sicherheitsverriegelt ist oder eine Sicherheits-Task-Signatur existiert, kann die in diesem Hinweis beschriebene Situation nicht auftreten. |

## Verwendung von HMI-Schnittstellen

Halten Sie die folgenden Vorsichtsmaßnahmen und Leitlinien für die Verwendung von HMI-Geräten in GuardLogix-Systemen mit SIL-Einstufung ein.

### Vorsichtsmaßnahmen

Sie müssen Vorsichtsmaßnahmen ergreifen und spezifische Techniken zu HMI-Geräten implementieren. Diese Vorsichtsmaßnahmen umfassen u. a.:

- Zugriffsbeschränkung und Sicherheit
- Spezifikationen, Tests und Validierung
- Beschränkungen hinsichtlich Daten und Zugriff
- Beschränkungen zu Daten und Parametern

Informationen dazu, wie sich HMI-Geräte in einem typischen SIL-Regelkreis nutzen lassen, finden Sie in Abbildung 1 auf Seite 15.

Nutzen Sie in der Anwendungssoftware des HMI und der Steuerung bewährte Techniken.

## Zugriff auf sicherheitstechnische Systeme

HMI-bezogene Funktionen bestehen aus zwei primären Aktivitäten: dem Lesen und dem Schreiben von Daten.

### *Parameter in sicherheitstechnischen Systemen lesen*

Das Lesen von Daten unterliegt keiner Beschränkung, da das Lesen keinen Einfluss auf das Verhalten des Sicherheitssystems hat. Allerdings können sich Zahl, Frequenz und Umfang der gelesenen Daten auf die Verfügbarkeit der Steuerung auswirken. Um sicherheitstechnische Fehlerauslösungen zu vermeiden, sollten Sie daher bewährte Kommunikationsverfahren nutzen, um die Auswirkungen der Kommunikationsverarbeitung auf die Steuerung zu begrenzen. Stellen Sie die Leseraten nicht auf die höchstmögliche Rate ein.

### *Parameter in SIL-bezogenen Systemen ändern*

Es ist nur unter folgenden Beschränkungen zulässig, Parameter in einem sicherheitstechnischen Regelkreis über ein externes Gerät zu ändern (d. h. ein Gerät, das sich außerhalb des Sicherheitsregelkreises befindet, wie z. B. ein HMI):

- Nur entsprechend autorisierte, speziell geschulte Mitarbeiter (Bediener) dürfen über eine Bedienerschnittstelle die Parameter in sicherheitstechnischen Systemen ändern.
- Der Bediener, der über ein HMI Änderungen in einem sicherheitstechnischen System vornimmt, ist für die Auswirkungen verantwortlich, die diese Änderungen auf den Sicherheitsregelkreis haben.
- Sie müssen alle Variablen, die geändert werden sollen, deutlich dokumentieren.
- Sie müssen eine klare, umfassende und explizite Bedienerverfahrensvorschrift nutzen, um über ein HMI sicherheitstechnische Änderungen vorzunehmen.
- Änderungen können in einem sicherheitstechnischen System nur dann akzeptiert werden, wenn die nachfolgende Abfolge von Ereignissen eingehalten wird:
    a. Die neue Variable muss zweimal an zwei verschiedene Tags gesendet werden; d. h., die beiden Werte dürfen nicht mit einem Befehl geschrieben werden.
    b. Der sicherheitstechnische Code, der in der Steuerung ausgeführt wird, muss beide Tags auf Äquivalenz prüfen und sicherstellen, dass sie innerhalb des zulässigen Bereichs liegen (Überprüfung der Grenzen).
    c. Die beiden neuen Variablen müssen zurückgelesen und auf dem HMI-Gerät angezeigt werden.
    d. Geschulte Bediener müssen anhand einer Sichtprüfung sicherstellen, dass die beiden Variablen gleich sind und den korrekten Wert aufweisen.

e. Geschulte Bediener müssen manuell quittieren, dass die Werte auf dem HMI-Bildschirm, der einen Befehl an die Sicherheitslogik sendet, wodurch die neuen Werte in der Sicherheitsfunktion verwendet werden können, korrekt sind.

In jedem Fall muss der Bediener die Gültigkeit der Änderungen bestätigen, bevor sie im Sicherheitsregelkreis akzeptiert und übernommen werden.

- Test aller Änderungen im Rahmen der Sicherheitsvalidierung.
- Ausreichende Dokumentation aller sicherheitstechnischen Änderungen, die über die Bedienerschnittstelle vorgenommen wurden, einschließlich:
  - Berechtigung
  - Einflussanalyse
  - Ausführung
  - Testinformationen
  - Versionsinformationen
- Änderungen am sicherheitstechnischen System müssen die IEC 61511-Norm zur Prozesssicherheit, Abschnitt 11.7.1 Anforderungen an Bedienerschnittstellen, erfüllen.
- Änderungen am sicherheitstechnischen System müssen die IEC 62061-Norm zur Maschinensicherheit erfüllen.
- Der Entwickler muss die gleichen bewährten Entwicklungstechniken und Verfahrensvorschriften einhalten wie bei der Entwicklung anderer Anwendungssoftware. Das schließt auch das Verifizieren und Testen der Bedienerschnittstelle und ihres Zugriffs auf andere Programmteile ein. Erstellen Sie in der Anwendungssoftware der Steuerung eine Tabelle, die für die Bedienerschnittstelle zugänglich ist, und beschränken Sie den Zugriff auf die erforderlichen Datenpunkte.
- Nachdem das System validiert und getestet wurde, muss die HMI-Software – ähnlich wie das Steuerprogramm – zur Einhaltung der SIL-Einstufung gesichert und gepflegt werden.

## Sicherheitsprogramme

Ein Sicherheitsprogramm verfügt über alle Eigenschaften eines Standardprogramms, lässt sich aber nur in der Sicherheits-Task planen. Ein Sicherheitsprogramm kann auch Sicherheits-Tags im Programmbereich definieren. Ein Sicherheitsprogramm kann zyklisch oder azyklisch ausgeführt werden.

Ein Sicherheitsprogramm kann nur Sicherheitskomponenten enthalten. Alle Routinen in einem Sicherheitsprogramm sind Sicherheitsroutinen. Ein Sicherheitsprogramm kann keine Standardroutinen oder Standard-Tags enthalten.

## Sicherheitsroutinen

Eine Sicherheitsroutine verfügt über alle Eigenschaften einer Standardroutine, kann jedoch nur in einem Sicherheitsprogramm existieren. Eine Sicherheitsroutine kann als Hauptroutine festgelegt werden. Eine andere Sicherheitsroutine kann als Fehlerroutine festgelegt werden. Nur Sicherheitsbefehle können in Sicherheitsroutinen verwendet werden.

Eine Auflistung der Befehle für die Sicherheitsanwendung finden Sie in Anhang A.



**ACHTUNG:** Damit SIL 3 eingehalten wird, müssen Sie sicherstellen, dass Ihre Sicherheitslogik nicht versucht, Standard-Tags zu lesen oder zu schreiben.

## Sicherheits-Tags

Das Steuerungssystem GuardLogix unterstützt den Einsatz von Standard- und Sicherheits-Tags im gleichen Projekt. Die Programmiersoftware unterscheidet jedoch in betrieblicher Hinsicht zwischen Standard- und Sicherheits-Tags.

Sicherheits-Tags besitzen alle Eigenschaften von Standard-Tags sowie Mechanismen zur Sicherung der SIL 3-Datenintegrität.

**Tabelle 6 – Gültige Datentypen für Sicherheits-Tags**

| | | |
|---|---|---|
| • AUX_VALVE_CONTROL | • DINT | • MUTING_FOUR_SENSOR_BIDIR |
| • BOOL | • DIVERSE_INPUT | • MUTING_TWO_SENSOR_ASYM |
| • CAM_PROFILE | • EIGHT_POS_MODE_SELECTOR | • MUTING_TWO_SENSOR_SYM |
| • CAMSHAFT_MONITOR | • EMERGENCY_STOP | • MOTION_INSTRUCTION |
| • CB_CONTINUOUS_MODE | • ENABLE_PENDANT | • PHASE |
| • CB_CRANKSHAFT_POS_MONITOR | • EXT_ROUTINE_CONTROL | • PHASE_INSTRUCTION |
| • CB_INCH_MODE | • EXT_ROUTINE_PARAMETERS | • REAL |
| • CB_SINGLE_STROKE_MODE | • FBD_BIT_FIELD_DISTRIBUTE | • REDUNDANT_INPUT |
| • CONFIGURABLE_ROUT | • FBD_CONVERT | • REDUNDANT_OUTPUT |
| • CONNECTION_STATUS | • FBD_COUNTER | • SAFETY_MAT |
| • CONTROL | • FBD_LOGICAL | • SERIAL_PORT_CONTROL |
| • COUNTER | • FBD_MASK_EQUAL | • SFC_ACTION |
| • DCA_INPUT | • FBD_MASKED_MOVE | • SFC_STEP |
| • DCI_MONITOR | • FBD_TIMER | • SFC_STOP |
| • DCI_START | • FIVE_POS_MODE_SELECTOR | • SINT |
| • DCI_STOP | • INT | • STRING |
| • DCI_STOP_TEST | • LIGHT_CURTAIN | • THRS_ENHANCED |
| • DCI_STOP_TEST_LOCK | • MAIN_VALVE_CONTROL | • TIMER |
| • DCI_STOP_TEST_MUTE | • MANUAL_VALVE_CONTROL | • TWO_HAND_RUN_STATION |

Die Anwendung Logix Designer verhindert die direkte Erzeugung von ungültigen Tags in einem Sicherheitsprogramm. Wenn Sie ungültige Tags importieren, können diese nicht verifiziert werden.

| **WICHTIG** | Aliasing zwischen Standard- und Sicherheits-Tags ist in Sicherheitsanwendungen nicht zulässig. |
|---|---|

Als Sicherheits-Tags klassifizierte Tags werden entweder im Steuerungsbereich oder im Sicherheitsprogrammbereich ausgeführt. Sicherheits-Tags im Steuerungsbereich können von jeder Standard- oder Sicherheitslogik oder von anderen Kommunikationsgeräten gelesen, jedoch nur durch Sicherheitslogik oder eine andere GuardLogix-Sicherheitssteuerung geschrieben werden. Auf Sicherheits-Tags im Programmbereich kann nur durch die lokalen Sicherheitsroutinen zugegriffen werden. Hierbei handelt es sich um Routinen, die sich innerhalb des Sicherheitsprogramms befinden.

Mit Sicherheits-E/A verknüpfte Tags und produzierte oder konsumierte Sicherheitsdaten müssen Tags im Sicherheitssteuerungsbereich sein.

| | |
|---|---|
| **WICHTIG** | Jedes Sicherheits-Tag im Steuerungsbereich kann von jeder Standardroutine gelesen werden, wobei die Aktualisierungsgeschwindigkeit von der Ausführung der Sicherheits-Task abhängt. Daher werden Sicherheits-Tags mit der periodischen Geschwindigkeit der Sicherheits-Task aktualisiert. Dieses Verhalten unterscheidet sich von dem der Standard-Tags. |

## Verwendung von Standard-Tags in Sicherheitsroutinen (Tag-Zuordnung)

Standard-Tags im Steuerungsbereich können Sicherheits-Tags zugewiesen werden, sodass ein Mechanismus zur Synchronisierung von Standard- und Sicherheitsaktionen zur Verfügung steht.



**ACHTUNG:** Bei Verwendung von Standarddaten in einer Sicherheitsroutine sind Sie dafür verantwortlich, eine zuverlässige Methode zur sicheren Verwendung der Daten bereitzustellen. Wenn Sie Standarddaten in einem Sicherheits-Tag verwenden, werden diese nicht zu Sicherheitsdaten. Sie dürfen einen Sicherheitsausgang mit Standard-Tag-Daten nicht direkt steuern.

Dieses Beispiel veranschaulicht, wie die Standarddaten mit Sicherheitsdaten beschrieben werden können.

**Abbildung 14 – Beschreiben von Standarddaten mit Sicherheitsdaten**

Safety Tag Mapping
Standard Tag Name | Safety Tag Name
STDBooleanTag | MappedBooleanTag
Close
Help
Delete Row

MappedBooleanTag
LatchOneShot
ONS
Node30ComboModule:I.Pt07Data
Node30ComboModule:O.Pt03Data
Node30ComboModule:O.Pt03Data

Sicherheitseingangsqualifikator für zugeordnetes Tag

Verriegelungsschaltung zur Vermeidung eines automatischen Neustarts, wenn der Standardeingang (MappedTag) mit dem Zustand „liegt ständig auf 1“ ausgefallen ist.

Sicherheitsausgang

# Notizen:

# Entwicklung von Sicherheitsanwendungen



## Voraussetzungen für das Sicherheitskonzept

Das Sicherheitskonzept geht davon aus, dass:

- es sich bei den für das Erstellen, den Betrieb und die Pflege der Anwendung Verantwortlichen um umfassend qualifiziertes, speziell geschultes Personal handelt, das über Erfahrung im Einsatz von Sicherheitssystemen verfügt.
- der Anwender die Logik korrekt anwendet, d. h. Programmierfehler erkannt werden. Programmierfehler können durch die strikte Einhaltung von Spezifikationen, Programmier- und Benennungsregeln erkannt werden.
- der Anwender seine Applikation einer kritischen Analyse unterzieht und alle möglichen Maßnahmen zur Ausfallerkennung nutzt.
- der Anwender sämtliche Downloads der Applikation mittels manueller Überprüfung der Sicherheits-Task-Signatur bestätigt.
- das gesamte System vor der ersten Inbetriebnahme eines sicherheitstechnischen Systems einer vollständigen Funktionsprüfung unterzogen wird.

**Tabelle 7 – Steuerungsmodi**

| Steuerungs-modus | Status Sicherheits-Task | Sicherheit[1] (bis einschl.) | Kommentare (Es wurde ein gültiges Programm in die Steuerung heruntergeladen.) |
|---|---|---|---|
| Programm | Entriegelt<br>Keine Signatur | | • E/A-Verbindungen hergestellt.<br>• Logik der Sicherheits-Task wird nicht gescannt. |
| Run | Entriegelt<br>Keine Signatur | (nur zu Entwicklungszwecken) | • Force-Zustände sind zulässig.<br>• Online-Bearbeitung ist zulässig.<br>• Sicherheitsspeicher ist isoliert, aber ungeschützt (Lesen/Schreiben).<br>• Logik der Sicherheits-Task wird gescannt.<br>Primär- und Partnersteuerung verarbeiten Logik, vergleichen Logikausgänge. Logikausgänge werden zu Sicherheitsausgängen geschrieben. |
| Run | Verriegelt<br>Keine Signatur | PLd/Cat. 3<br>Steuerung zuverlässig<br>SIL CL2 | • Neue Force-Zustände sind nicht zulässig. Bestehende Force-Zustände bleiben erhalten.<br>• Online-Bearbeitung ist nicht zulässig.<br>• Sicherheitsspeicher ist geschützt (nur Lesen).<br>• Logik der Sicherheits-Task wird gescannt.<br>• Primär- und Partnersteuerung verarbeiten Logik, vergleichen Logikausgänge. Logikausgänge werden zu Sicherheitsausgängen geschrieben. |
| Run | Entriegelt<br>Mit Signatur | Ple/Cat. 4<br>Steuerung zuverlässig<br>SIL CL3 | • Force-Zustände sind nicht zulässig. (Force-Zustände müssen zur Erzeugung einer Sicherheits-Task-Signatur entfernt werden.)<br>• Online-Bearbeitung ist nicht zulässig.<br>• Sicherheitsspeicher ist geschützt (nur Lesen).<br>• Logik der Sicherheits-Task wird gescannt.<br>• Primär- und Partnersteuerung verarbeiten Logik, vergleichen Logikausgänge. Logikausgänge werden zu Sicherheitsausgängen geschrieben.<br>• Sicherheits-Task-Signatur ist ungeschützt und kann von jedem Anwender mit Zugriff auf die Steuerung gelöscht werden. |
| Run | Verriegelt<br>Mit Signatur | Ple/Cat. 4<br>Steuerung zuverlässig<br>SIL CL3 | • Force-Zustände sind nicht zulässig. (Force-Zustände müssen zur Erzeugung einer Sicherheits-Task-Signatur entfernt werden.)<br>• Online-Bearbeitung ist nicht zulässig.<br>• Sicherheitsspeicher ist geschützt (nur Lesen).<br>• Logik der Sicherheits-Task wird gescannt.<br>• Primär- und Partnersteuerung verarbeiten Logik, vergleichen Logikausgänge. Logikausgänge werden zu Sicherheitsausgängen geschrieben.<br>• Sicherheits-Task-Signatur ist geschützt. Anwender müssen das Entriegelungskennwort eingeben, um die Steuerung zu entriegeln, bevor sie die Sicherheits-Task-Signatur löschen können. |

(1) Um diese Ebene zu erreichen, müssen Sie die in dieser Publikation definierten sicherheitstechnischen Anforderungen einhalten.

## Grundlagen der Anwendungsentwicklung und -prüfung

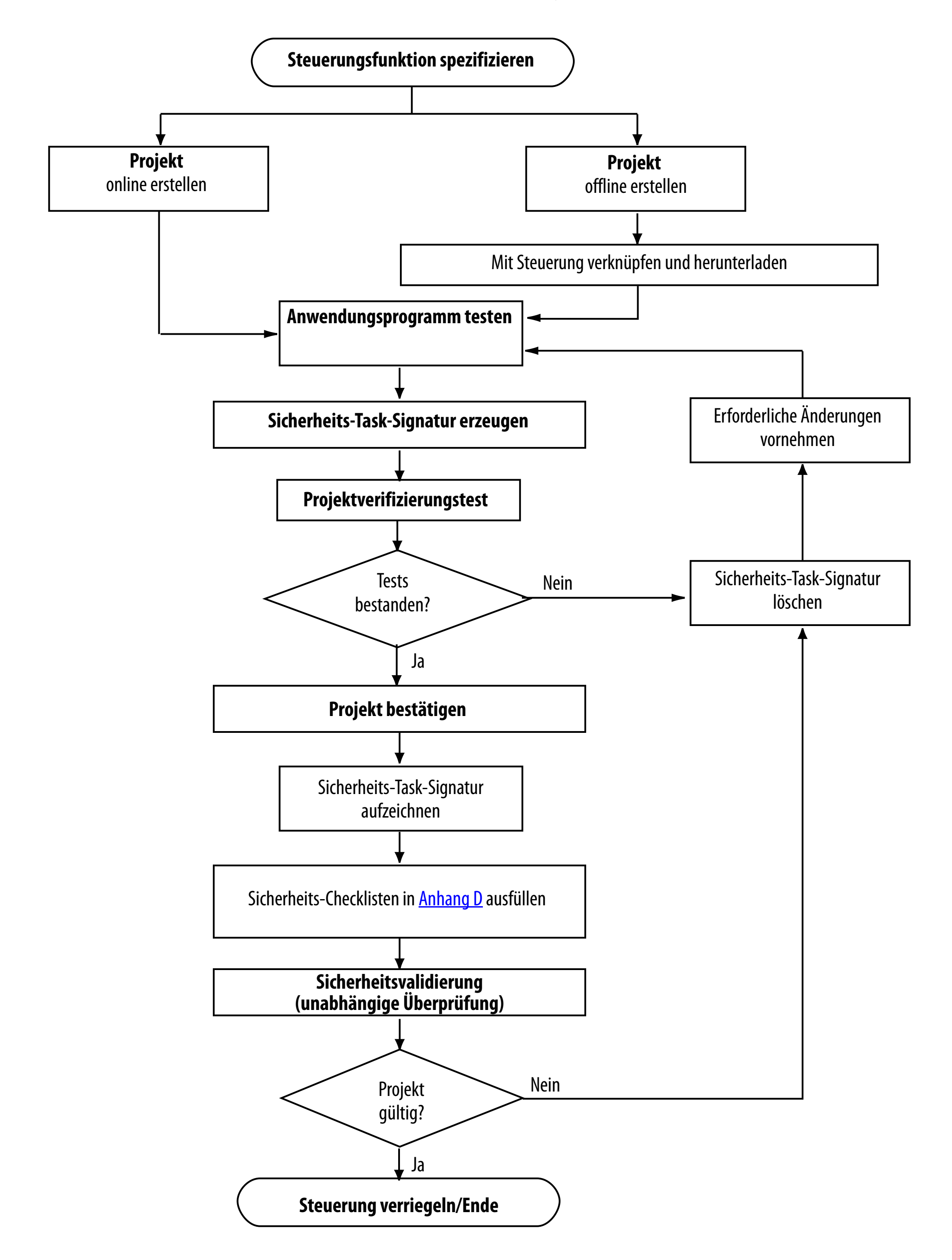
Das Anwendungsprogramm für das beabsichtigte SIL CL3-System sollte vom Systemintegrator und/oder einem Anwender mit Ausbildung und Erfahrung im Bereich der Sicherheitsanwendungen entwickelt werden. Der Entwickler muss eine fundierte Entwicklungspraxis aufweisen und in der Lage sein, Folgendes zu verwenden:

- Verwendung von Funktionsspezifikationen wie Flussdiagrammen, Zeitdiagrammen und Ablauftabellen
- Überprüfung der Sicherheits-Task-Logik
- Validierung der Anwendung

## Inbetriebnahme prozess

Das nachstehende Diagramm zeigt die zur Inbetriebnahme eines GuardLogix-Systems erforderlichen Schritte. Die Elemente in Fettdruck werden in den folgenden Abschnitten erklärt.

**Abbildung 15 – Inbetriebnahme des Systems**



## Steuerungsfunktion spezifizieren

Sie müssen eine Spezifikation für Ihre Steuerungsfunktion erstellen. Nutzen Sie diese Spezifikation, um zu bestätigen, dass die Programmlogik korrekt ist und die Funktions- und Sicherheitssteuerungsanforderungen Ihrer Anwendung vollständig erfüllt. Die Spezifikation kann, abhängig von Ihrer Applikation, in einer Vielzahl von Formaten präsentiert werden. Diese Spezifikation muss jedoch eine detaillierte Beschreibung beinhalten, zu der (sofern zutreffend) folgende Elemente gehören:

- Ablauffolge im Betrieb
- Fluss- und Zeitdiagramme
- Ablauftabellen
- Programmbeschreibung
- Programmausdruck
- In Worten formulierte Beschreibungen der Schritte mit den entsprechenden Bedingungen und zu steuernden Aktoren, inklusive:
  - Eingangsdefinitionen
  - Ausgangsdefinitionen
  - E/A-Verdrahtungspläne und -referenzen
  - Funktionstheorie
- Matrix oder Tabelle der Bedingungen für die einzelnen Schritte und der zu steuernden Aktoren, einschließlich Ablauf- und Zeitdiagrammen
- Definition der Randbedingungen, z. B. Betriebsarten, NOT-HALT usw.

Der E/A-Teil der Spezifikation muss die Analyse der Feldschaltkreise, d. h. den Typ der Sensoren und Aktoren enthalten.

- Sensoren (digital oder analog)
  - Signal im Standardbetrieb (Ruhestromprinzip für digitale Sensoren, Sensoren AUS bedeutet kein Signal)
  - Bestimmung der für SIL-Stufen erforderlichen Redundanzen
  - Diskrepanzüberwachung und -visualisierung einschließlich der Diagnoselogik des Anwenders
- Aktoren
  - Positionierung und Aktivierung im Standardbetrieb (normalerweise AUS)
  - Sichere Reaktion/Positionierung bei Ausschaltung oder Stromausfall
  - Diskrepanzüberwachung und -visualisierung einschließlich der Diagnoselogik des Anwenders

## Projekt erstellen

Logik und Befehle, die bei der Programmierung der Anwendung verwendet werden, müssen:

- einfach zu verstehen
- einfach zurückzuverfolgen
- einfach zu ändern
- einfach zu testen sein.

Überprüfen und testen Sie die gesamte Logik. Sicherheitsbezogene Logik und Standardlogik sind voneinander zu trennen.

*Programm kennzeichnen*

Das Anwendungsprogramm wird über eines der folgenden Elemente eindeutig identifiziert:

- Name
- Datum
- Version
- Jede andere Benutzeridentifikation

## Anwendungsprogramm testen

Dieser Schritt besteht aus einer Kombination aus Ausführungs- (RUN) und Programm-Modus, Online- oder Offline-Bearbeitungen, Hochladen und Herunterladen sowie informellem Testen, das erforderlich ist, um – zur Vorbereitung auf den Projektverifizierungstest – die korrekte Ausführung einer Anwendung zu erreichen.

## Sicherheits-Task-Signatur erzeugen

Die Sicherheits-Task-Signatur identifiziert jedes Projekt eindeutig, einschließlich seiner Logik, Daten und Konfiguration. Die Sicherheits-Task-Signatur besteht aus einer ID (Identifikationsnummer), Datum und Zeit.

Sie können die Sicherheits-Task-Signatur erzeugen, wenn alle folgenden Bedingungen zutreffen:

- die Anwendung Logix Designer ist mit der Steuerung online,
- die Steuerung befindet sich im Programmmodus,
- die Steuerung ist sicherheitsentriegelt,
- die Steuerung unterliegt keinen Sicherheits-Forcen oder anstehenden Online-Sicherheitsbearbeitungen und
- der Status der Sicherheits-Task ist OK.

Sobald die Prüfung des Anwendungsprogramms abgeschlossen ist, muss die Sicherheits-Task-Signatur erzeugt werden. Nach Erzeugung der Signatur wird diese von der Programmiersoftware automatisch hochgeladen.

| | |
|---|---|
| **WICHTIG** | Zur Überprüfung der Integrität jedes Download-Vorgangs müssen Sie die Sicherheits-Task-Signatur nach der ersten Erstellung manuell erfassen und die Sicherheits-Task-Signatur nach jedem Herunterladen prüfen, um sicherzustellen, dass sie dem Original entspricht. |

Sie können die Sicherheits-Task-Signatur nur dann löschen, wenn die GuardLogix-Steuerung nicht sicherheitsverriegelt ist und, wenn sie online ist, der Schlüsselschalter in der Position REM oder PROG steht.

Wenn eine Sicherheits-Task-Signatur vorhanden ist, sind die folgenden Aktionen in der Sicherheits-Task nicht gestattet:

- Online- oder Offline-Programmierung oder -Bearbeitung von Sicherheitskomponenten
- „Forcen" von Sicherheits-E/A
- Datenmanipulation (außer durch Routinelogik oder eine andere GuardLogix-Steuerung)

## Projektverifizierungstest

Um zu überprüfen, ob Ihr Anwendungsprogramm die Spezifikation einhält, müssen Sie eine geeignete, die Anwendung abdeckende Testreihe erstellen. Diese Testfälle müssen als Testspezifikation archiviert werden.

Sie müssen eine Reihe von Tests durchführen, die die Gültigkeit der in der Applikationslogik verwendeten Berechnungen (Formeln) bestätigen. Gleichwertige Bereichstests sind akzeptabel. Dabei handelt es sich um Tests innerhalb der definierten Wertbereiche, an den Grenzbereichen oder in ungültigen Wertbereichen. Die notwendige Anzahl von Testfällen hängt von den verwendeten Formeln ab und muss kritische Wertepaare umfassen.

Eine aktive Simulation mit Quellen (Feldgeräten) muss ebenfalls enthalten sein, da dies die einzige Möglichkeit darstellt, die korrekte Verdrahtung der Sensoren und Aktoren im System zu bestätigen. Prüfen Sie den Betrieb der programmierten Funktionen, indem Sie Sensoren und Aktoren manuell manipulieren.

Die Testreihe muss auch Tests zur Überprüfung der Reaktion auf Verdrahtungsstörungen und Netzwerkkommunikationsstörungen einschließen.

Die Projektverifizierung umfasst Tests von Fehlerroutinen, Eingangs- und Ausgangskanälen, mit deren Hilfe sichergestellt wird, dass das Sicherheitssystem ordnungsgemäß arbeitet.

Soll ein Projektverifizierungstest für die GuardLogix-Steuerung durchgeführt werden, müssen Sie die Anwendung einem vollständigen Test unterziehen. Sie müssen alle Sensoren und Aktoren jeder einzelnen Sicherheitsfunktion umschalten. Aus der Sicht der Steuerung bedeutet dies, dass der E/A-Punkt zur Steuerung umgeschaltet wird, also nicht unbedingt die tatsächlichen Aktoren. Vergewissern Sie sich, dass Sie alle Abschaltfunktionen testen, da

diese Funktionen in der Regel während des normalen Betriebs nicht ausgeführt werden. Bedenken Sie außerdem, dass ein Projektverifizierungstest nur für die jeweils getestete Anwendung gültig ist. Wird die Steuerung auf eine andere Anwendung verlagert, müssen Sie die Steuerung einem Inbetriebnahme- und einem Projektverifizierungstest im Zusammenhang mit dem neuen Anwendungsprogramm unterziehen.

## Projekt bestätigen

Sie müssen das Projekt ausdrucken oder anzeigen und die hochgeladenen Sicherheits-E/A- und Steuerungskonfigurationen, Sicherheitsdaten sowie Programmlogik der Sicherheits-Task manuell vergleichen, um sicherzustellen, dass die richtigen Sicherheitskomponenten heruntergeladen, getestet und im Sicherheitsanwendungsprogramm gespeichert wurden.

Falls Ihr Anwendungsprogramm einen Sicherheits-Add-On-Befehl enthält, der mit einer Befehlssignatur abgeschlossen (versiegelt) wurde, dann müssen Sie auch die Befehlssignatur, Datum/Uhrzeit und die Sicherheitsbefehlssignatur mit den Werten vergleichen, die Sie beim Abschließen des Add-On-Befehls aufgezeichnet haben.

Informationen dazu, wie Sie Sicherheits-Add-On-Befehle in SIL 3-Anwendungen erstellen und verwenden, finden Sie in Anhang B, Sicherheits-Add-On-Befehle.

Die nachstehenden Schritte zeigen ein Verfahren zur Bestätigung des Projekts:

1. Speichern Sie das Projekt, während sich die Steuerung im Programmmodus befindet.
2. Beantworten Sie die Frage nach dem Hochladen der Tag-Werte mit „Ja“.
3. Speichern Sie, während die Anwendung Logix Designer offline ist, das Projekt unter einem neuen Namen wie etwa „Offline-Projektname.ACD“, wobei „Projektname“ der Name Ihres Projekts ist.

   Hierbei handelt es sich nun um die neue getestete Master-Projektdatei.
4. Schließen Sie das Projekt.
5. Verschieben Sie die Archivdatei mit dem Originalprojekt aus ihrem aktuellen Verzeichnis.
   Sie können diese Datei löschen oder an einer entsprechenden Stelle speichern (Archiv). Dieser Schritt ist erforderlich, denn wenn die Anwendung Logix Designer die Datei Projektname.ACD in diesem Verzeichnis findet, dann setzt sie sie mit dem Steuerungsprojekt in Beziehung und führt keinen aktuellen Upload durch.
6. Belassen Sie die Steuerung weiterhin im Programmmodus und laden Sie das Projekt von der Steuerung hoch.
7. Speichern Sie das hochgeladene Projekt unter dem Namen „Online-Projektname.ACD“, wobei Projektname der Name Ihres Projekts ist.
8. Beantworten Sie die Frage nach dem Hochladen der Tag-Werte mit „Ja“.

9. Verwenden Sie das Dienstprogramm „Program Compare“ von Logix Designer, um die folgenden Vergleiche durchzuführen:
   - Vergleichen Sie alle Eigenschaften der GuardLogix-Steuerung und der CIP Safety-E/A-Geräte.
   - Vergleichen Sie alle Eigenschaften der Sicherheits-Task, Sicherheitsprogramme und Sicherheitsroutinen.
   - Vergleichen Sie die gesamte Logik in den Sicherheitsroutinen.

## Sicherheitsvalidierung

Eine unabhängige Überprüfung des Sicherheitssystems durch einen Dritten ist ggf. erforderlich, bevor das System zum Betrieb freigegeben wird. Eine unabhängige Zertifizierung durch einen Dritten ist für IEC 61508 SIL 3 erforderlich.

## GuardLogix-Steuerung verriegeln

Das GuardLogix-Steuerungssystem kann sicherheitsverriegelt werden, um Komponenten der Sicherheitssteuerung vor Änderung zu schützen. Die Sicherheitsverriegelung der Steuerung ist jedoch keine Anforderung für SIL 3-Anwendungen. Die Funktion der Sicherheitsverriegelung gilt nur für Sicherheitskomponenten wie z. B. die Sicherheits-Task, Sicherheits-Programme, Sicherheits-Routinen, Sicherheits-Tags, Sicherheits-Add-On-Befehle, E/A-Sicherheitsmodule und die Sicherheits-Task-Signatur. Die Sicherheitsverriegelung allein erfüllt jedoch nicht die Anforderungen von SIL 3.

Kein Teil der Sicherheit kann geändert werden, während sich die Steuerung im sicherheitsverriegelten Zustand befindet. Wenn die Steuerung sicherheitsverriegelt ist, sind die folgenden Aktionen in der Sicherheits-Task nicht gestattet:

- Online- oder Offline-Programmierung oder -Bearbeitung
- „Forcen“ von Sicherheits-E/A
- Datenmanipulation (außer durch Routinelogik oder eine andere GuardLogix-Steuerung)
- Erstellen oder Bearbeiten von Sicherheits-Add-On-Befehlen
- Erzeugen oder Löschen der Sicherheits-Task-Signatur

Der Standardzustand der Steuerung ist sicherheitsentriegelt. Sie können die Sicherheitsanwendung unabhängig davon, ob Sie online oder offline sind, und ungeachtet dessen, ob Sie über die Originalquelle des Programms verfügen, in den sicherheitsverriegelten Zustand setzen. Es dürfen jedoch keine Sicherheits-Forces oder anstehenden Sicherheitsbearbeitungen vorliegen. Der Status „sicherheitsverriegelt“ bzw. „sicherheitsentriegelt“ kann nicht geändert werden, wenn der Schlüsselschalter in der Stellung RUN steht.

Als zusätzlicher Schutz können getrennte Kennwörter für die Sicherheitsverriegelung und -entriegelung der Steuerung verwendet werden.
Die Verwendung von Kennwörtern ist optional.

## Herunterladen eines Sicherheitsanwendungs-programms

Beim Herunterladen ist ein Anwendungstest erforderlich, sofern keine Sicherheits-Task-Signatur existiert.

| | |
|---|---|
| **WICHTIG** | Zur Überprüfung der Integrität jedes Download-Vorgangs müssen Sie die Sicherheits-Task-Signatur nach der ersten Erstellung manuell erfassen und die Sicherheits-Task-Signatur nach jedem Herunterladen prüfen, um sicherzustellen, dass sie dem Original entspricht. |

Der Download auf eine sicherheitsverriegelte GuardLogix-Steuerung ist nur zulässig, wenn die Sicherheits-Task-Signatur, die Hardwareserie und die Betriebssystemversion des Offline-Projekts mit den in der GuardLogix-Zielsteuerung enthaltenen übereinstimmt und der Status der Sicherheits-Task „OK" ist.

| | |
|---|---|
| **WICHTIG** | Falls die Sicherheits-Task-Signatur nicht übereinstimmt und die Steuerung sicherheitsverriegelt ist, müssen Sie die Steuerung für den Download-Vorgang entriegeln. In diesem Fall wird die Sicherheits-Task-Signatur durch den Download auf die Steuerung gelöscht. Daher müssen Sie die Anwendung erneut validieren. |



**ACHTUNG:** Der USB-Port ist nur zur temporären lokalen Programmierzwecken gedacht und nicht für einen permanenten Anschluss.

## Hochladen eines Sicherheits-anwendungsprogramms

Enthält die GuardLogix-Steuerung eine Sicherheits-Task-Signatur, wird die Sicherheits-Task-Signatur mit dem Projekt hochgeladen. Dies bedeutet, dass alle an den Offline-Sicherheitsdaten vorgenommenen Änderungen beim Upload überschrieben werden.

## Online-Bearbeitung

Falls keine Sicherheits-Task-Signatur vorhanden ist und die Steuerung sicherheitsentriegelt ist, können Sie Online-Bearbeitungen an Ihren Sicherheitsroutinen vornehmen.

| | |
|---|---|
| **TIPP** | Sie können keine Standard- oder Sicherheits-Add-On-Befehle bearbeiten, während Sie online sind. |

Anstehende Bearbeitungen können nicht vorgenommen werden, wenn die Steuerung sicherheitsverriegelt ist oder wenn eine Sicherheits-Task-Signatur vorhanden ist. Online-Bearbeitungen sind möglich, wenn die Steuerung sicherheitsverriegelt ist. Sie dürfen jedoch nicht assembliert oder gelöscht werden.

| | |
|---|---|
| **TIPP** | Online-Bearbeitungen in Standardroutinen sind vom sicherheits-verriegelten oder -entriegelten Zustand nicht betroffen. |

Weitere Informationen dazu, wie Sie Ihr Anwendungsprogramm bearbeiten, finden Sie auf Seite 59.

## Speichern und Laden eines Projektes aus einem nichtflüchtigen Speicher

Die Steuerungen der Serie GuardLogix 5570 unterstützen Firmware-Upgrades sowie das Speichern und Abrufen von Anwenderprogrammen mithilfe einer Speicherkarte. In einem GuardLogix-System verwendet nur die Primärsteuerung eine Speicherkarte für den nichtflüchtigen Speicher.

Wenn Sie ein Sicherheitsprojekt auf einer Speicherkarte speichern, dann empfiehlt Rockwell Automation Ihnen die Option „Remote Program" als „Load Mode" auszuwählen, d. h. der Modus, in den die Steuerung nach dem Laden wechselt. Vor dem eigentlichen Maschinenbetrieb ist der Eingriff des Bedieners erforderlich, um die Maschine zu starten.

Sie können den Ladevorgang aus dem nichtflüchtigen Speicher nur unter folgenden Bedingungen starten:

- Wenn der Typ der Steuerung, der durch das im nichtflüchtigen Speicher gespeicherte Projekt spezifiziert wird, mit dem Typ Ihrer Steuerung übereinstimmt.
- Wenn die größeren und kleineren Änderungen an dem im nichtflüchtigen Speicher gespeicherten Projekt mit den größeren und kleineren Änderungen an Ihrer Steuerung übereinstimmen.
- Wenn sich Ihre Steuerung nicht im Run-Modus befindet.

Es ist nur dann zulässig, ein Projekt in eine sicherheitsverriegelte Steuerung zu laden, wenn die Sicherheits-Task-Signatur des im nichtflüchtigen Speicher gespeicherten Projekts mit dem Projekt in der Steuerung übereinstimmt. Wenn die Signaturen nicht übereinstimmen oder wenn die Steuerung ohne Sicherheits-Task-Signatur sicherheitsverriegelt wurde, dann müssen Sie zuerst die Steuerung entriegeln, bevor Sie versuchen, die Steuerung über den nichtflüchtigen Speicher zu aktualisieren.

| | |
|---|---|
| **WICHTIG** | Wenn Sie die Steuerung entriegeln und den Ladevorgang aus dem nichtflüchtigen Speicher starten, dann werden – sobald der Ladevorgang abgeschlossen ist – der Status der Sicherheitsverriegelung, die Kennwörter und die Sicherheits-Task-Signatur auf die Werte gesetzt, die im nichtflüchtigen Speicher vorhanden sind. |

## Forcen

Alle in einem E/A, einem produzierten oder konsumierten Sicherheits-Tag (einschließlich CONNECTION_STATUS) enthaltenen Daten können einem Force unterzogen werden, während das Projekt sicherheitsentriegelt ist und keine Sicherheits-Task-Signatur existiert. Forces müssen jedoch bei allen Sicherheits-Tags deinstalliert, nicht nur deaktiviert, werden, bevor das Sicherheitsprojekt sicherheitsverriegelt oder eine Sicherheits-Task-Signatur erzeugt werden kann. Sie können keine Sicherheits-Tags forcen, während das Projekt sicherheitsverriegelt ist oder wenn eine Sicherheits-Task-Signatur vorhanden ist.

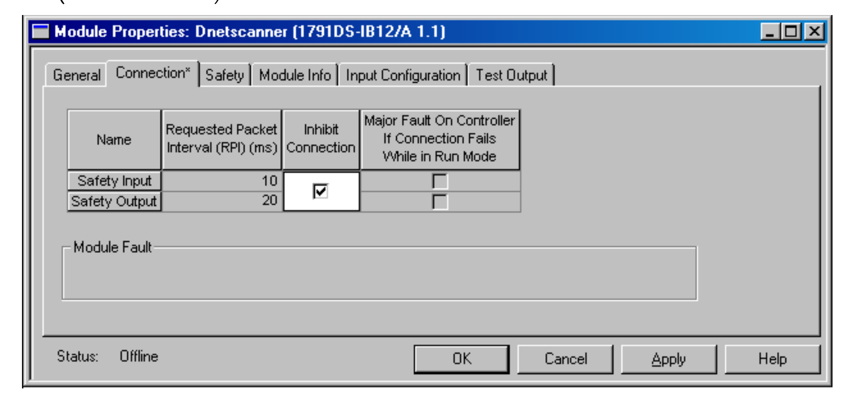
| | |
|---|---|
| **TIPP** | Sie können Forces bei Standard-Tags unabhängig vom sicherheitsverriegelten oder -entriegelten Zustand installieren und deinstallieren. |

## Sperren eines Geräts

Sie können CIP Safety-E/A-Geräte oder Producer-Steuerungen nicht sperren oder entsperren, wenn das Anwendungsprogramm sicherheitsverriegelt ist oder eine Sicherheits-Task-Signatur existiert.

Folgendes Vorgehen führt zum Sperren eines Sicherheits-E/A-Geräts:

1. Klicken Sie in der Anwendung Logix Designer mit der rechten Maustaste auf das Gerät und wählen Sie „Properties“ (Eigenschaften) aus.
2. Im Dialogfeld „Module Properties“ (Moduleigenschaften) auf die Registerkarte „Connection“ (Verbindung) klicken.
3. „Inhibit Connection“ (Verbindung sperren) markieren und auf „Apply“ (Übernehmen) klicken.




Das Gerät ist gesperrt, sobald das Kontrollkästchen aktiviert wurde. Falls ein Kommunikationsgerät gesperrt wurde, sind auch alle nachfolgenden Geräte gesperrt.

## Bearbeiten Ihrer Sicherheitsanwendung

Die folgenden Regeln gelten für das Ändern Ihres Sicherheitsanwendungs-programms in der Anwendung Logix Designer:

- Nur befugtes, speziell geschultes Personal kann Programmbearbeitungen vornehmen. Dieses Personal sollte alle verfügbaren übergeordneten Verfahren anwenden, z. B. den Schlüsselschalter der Steuerung oder den Sicherheitskennwortschutz nutzen.
- Wenn befugtes, speziell geschultes Personal Programmbearbeitungen vornimmt, übernehmen sie die zentrale Sicherheitsverantwortung, während die Änderungen vorgenommen werden. Dieses Personal muss ebenfalls sicheren Applikationsbetrieb aufrechterhalten.
- Bei der Online-Bearbeitung müssen Sie einen alternativen Schutzmechanismus anwenden, um die Sicherheit des Systems aufrechtzuerhalten.
- Sie müssen alle Programmbearbeitungen ausreichend dokumentieren, inklusive:
  - Berechtigung
  - Einflussanalyse
  - Ausführung
  - Testinformationen
  - Versionsinformationen
- Falls Online-Bearbeitungen nur in den Standardroutinen vorgenommen wurden, müssen diese Änderungen nicht validiert werden, bevor zum normalen Betrieb zurückgekehrt werden kann.

- Sie müssen sicherstellen, dass Änderungen an der Standardroutine im Hinblick auf Zeitsteuerung und Tag-Zuordnung für Ihre Sicherheitsanwendung akzeptabel sind.
- Sie **können** den Logikteil Ihres Programms wie in den folgenden Abschnitten beschrieben bearbeiten, während Sie offline oder online sind.

## Durchführen von Offline-Bearbeitungen

Wenn Offline-Bearbeitungen nur an Elementen des Standardprogramms vorgenommen werden und die Sicherheits-Task-Signatur nach einem Herunterladen übereinstimmt, können Sie den Betrieb wieder aufnehmen.

Wenn sich die Offline-Bearbeitung auf das Sicherheitsprogramm auswirkt, müssen Sie alle betroffenen Elemente der Anwendung – wie von der Einflussanalyse festgelegt – erneut validieren, bevor Sie den Betrieb wieder aufnehmen können.

Das Flussdiagramm auf Seite 61 zeigt das Verfahren zur Offline-Bearbeitung.

## Durchführen von Online-Bearbeitungen

Wenn sich die Online-Bearbeitung auf das Sicherheitsprogramm auswirkt, müssen Sie alle betroffenen Elemente der Anwendung – wie von der Einflussanalyse festgelegt – erneut validieren, bevor Sie den Betrieb wieder aufnehmen können. Das Flussdiagramm auf Seite 61 zeigt das Verfahren zur Online-Bearbeitung.

| TIPP | Beschränken Sie Online-Bearbeitungen auf kleinere Programmänderungen wie Sollwertänderungen oder kleine Logikergänzungen, -löschungen und -änderungen. |
|---|---|

Online-Bearbeitungen sind von den Funktionen Sicherheitsverriegelung und Sicherheits-Task-Signatur der GuardLogix-Steuerung betroffen.

Weitere Informationen finden Sie unter Sicherheits-Task-Signatur erzeugen auf Seite 53 und unter GuardLogix-Steuerung verriegeln auf Seite 56.

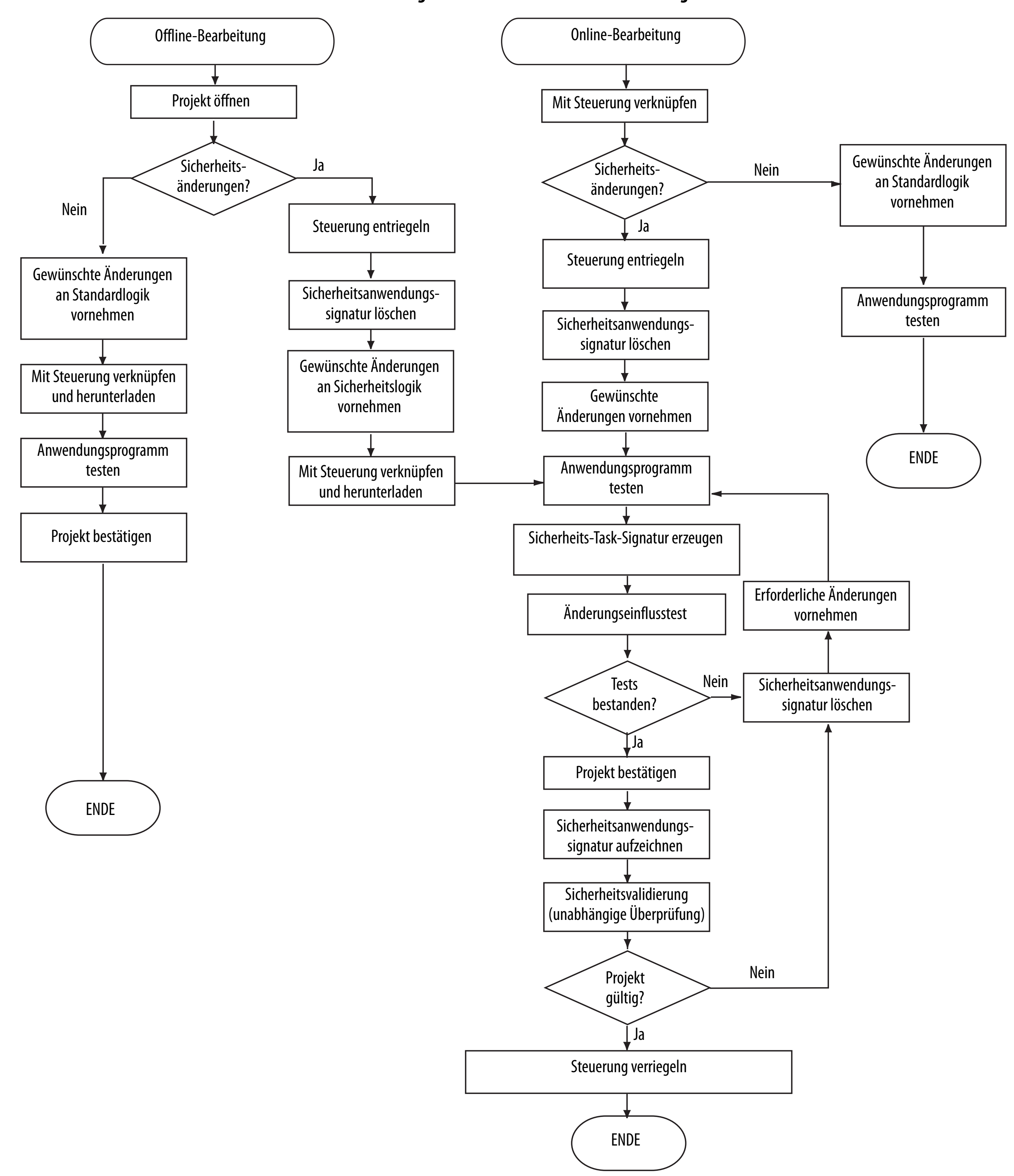
Detaillierte Informationen zur Online-Bearbeitung der Kontaktplanlogik in der Anwendung Logix Designer entnehmen Sie der Kurzanleitung „Steuerungen Logix5000, Schnellstart“, Publikation 1756-QS001.

## Änderungseinflusstest

Jede Änderung, Erweiterung oder Anpassung Ihrer validierten Software muss geplant und der Einfluss auf das funktionale Sicherheitssystem analysiert werden. Alle entsprechenden Phasen des Software-Sicherheitslebenszyklus müssen wie in der Einflussanalyse angegeben durchgeführt werden.
So muss die gesamte betroffene Software mindestens einem Funktionstest unterzogen werden. Alle Änderungen an Ihren Software-Spezifikationen sind

zu dokumentieren. Die Testergebnisse müssen ebenfalls dokumentiert werden. Detaillierte Informationen hierzu finden Sie in der IEC 61508-3, Abschnitt 7.8 Software-Modifikation.

**Abbildung 16 – Online- und Offline-Bearbeitungsverfahren**



# Notizen:

# Überwachung des Status und Handhabung von Störungen



Die GuardLogix-Architektur bietet dem Anwender viele Wege, Störungen im System zu erkennen und darauf zu reagieren. Die erste Möglichkeit zur Handhabung von Störungen durch den Anwender besteht darin, sicherzustellen, dass die Checklisten für die Applikation ausgefüllt wurden (siehe Anhang D).

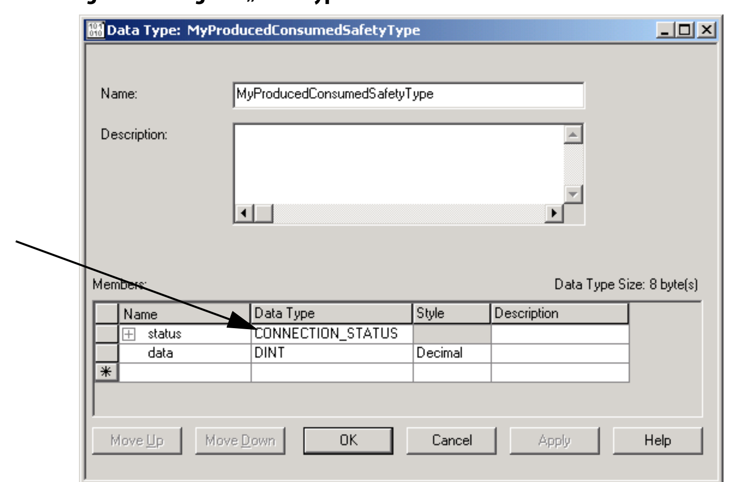
## Überwachen des Systemstatus

Sie können den Status der Sicherheits-Tag-Verbindungen abrufen. Sie können den aktuellen Betriebsstatus ebenfalls bestimmen, indem Sie verschiedene Geräteobjekte abfragen. Es liegt an Ihnen zu bestimmen, welche Daten am besten zur Einleitung einer Abschaltfolge geeignet sind.

### CONNECTION_STATUS-Daten

Das erste Glied der Tag-Struktur, das mit Sicherheitseingangsdaten und produzierten/konsumierten Sicherheits-Tag-Daten verknüpft ist, enthält den Status der Verbindung. Dieses Glied ist ein vordefinierter Datentyp mit dem Namen CONNECTION_STATUS.

**Abbildung 17 – Dialogfeld „Data Type“**



Die ersten beiden Bits des Datentyps CONNECTION_STATUS enthalten die Statusbits „RunMode" und „ConnectionFaulted" eines Geräts. Die folgende Tabelle beschreibt die Kombinationen der Zustände „RunMode" und „ConnectionFaulted".

**Tabelle 8 – Sicherheitsverbindungsstatus**

| RunMode-Status | ConnectionFaulted-Status | Betrieb der Sicherheitsverbindung |
|---|---|---|
| 1 = Run | 0 = Gültig | Daten werden aktiv durch das produzierende Gerät gesteuert. Das produzierende Gerät befindet sich im Run-Modus. |
| 0 = Leerlauf | 0 = Gültig | Die Verbindung ist aktiv und das produzierende Gerät ist im Leerlauf. Die Sicherheitsdaten werden auf null zurückgesetzt. |
| 0 = Leerlauf | 1 = Fehlerhaft | Die Sicherheitsverbindung ist fehlerhaft. Der Zustand des produzierenden Geräts ist unbekannt. Die Sicherheitsdaten werden auf null zurückgesetzt. |
| 1 | 1 | Ungültiger Zustand. |



**ACHTUNG:** Sicherheits-E/A-Verbindungen und produzierte/konsumierte Verbindungen können nicht automatisch dafür konfiguriert werden, die Steuerung in den Störungsstatus zu versetzen, wenn die Verbindung unterbrochen wird und das System in den sicheren Zustand übergeht. Falls Sie also eine Gerätestörung ermitteln müssen, um sicherzustellen, dass das System SIL 3 beibehält, müssen Sie die CONNECTION_STATUS-Bits der Sicherheits-E/A überwachen und die Störung über die Programmierlogik einleiten.

## Eingangs- und Ausgangsdiagnose

Guard I/O-Module stellen Impulstest- und Überwachungsfunktionen bereit. Wenn das Modul einen Fehler erkennt, wird der jeweilige Ein- oder Ausgang in den sicheren Zustand gesetzt und der Ausfall wird der Steuerung gemeldet. Die Ausfallanzeige erfolgt über den Ein- oder Ausgangspunktstatus und wird über einen konfigurierbaren Zeitraum beibehalten oder bis die Störung behoben wird.

**WICHTIG** Eine Kontaktplanlogik muss in das Anwendungsprogramm integriert werden, um E/A bei Punktausfall zu verriegeln und einen sicheren Neustart zu gewährleisten.

## Verbindungsstatus der E/A-Geräte

Das CIP Safety-Protokoll liefert den Status zu jedem E/A-Gerät im Sicherheitssystem. Wenn ein Eingangsverbindungsfehler erkannt wird, setzt das Betriebssystem alle Geräteeingänge in den ausgeschalteten (sicheren) Zustand und meldet den Ausfall der Kontaktplanlogik. Wird ein Ausfall der Ausgangsverbindung erkannt, kann das Betriebssystem den Ausfall nur an die Kontaktplanlogik berichten. Die Ausgänge werden durch das Ausgangsgerät deaktiviert.

**WICHTIG** Eine Kontaktplanlogik muss in das Anwendungsprogramm integriert werden, um E/A bei Punktausfall zu verriegeln und einen sicheren Neustart zu gewährleisten.

## Ruhestromprinzip-System

Die GuardLogix-Steuerungen sind Teil eines Ruhestromprinzip-Systems, d. h. eines Systems, bei dem null der sichere Zustand ist. Einige (aber nicht alle) Fehler im Sicherheits-E/A-Gerät führen dazu, dass alle Geräteeingänge oder -ausgänge auf null gesetzt werden (sicherer Zustand). Fehler, die einen spezifischen Eingangskanal betreffen, führen dazu, dass dieser spezifische Kanal auf null gesetzt wird. Ein Beispiel: Ein Impulstestfehler, der spezifisch Kanal 0 betrifft, führt dazu, dass die Eingangsdaten von Kanal 0 in den sicheren Zustand (0) versetzt werden. Wenn ein Fehler das Gerät im Allgemeinen betrifft und nicht nur einen spezifischen Kanal, dann zeigt das kombinierte Status-Bit den Fehlerstatus an, und alle Gerätedaten werden in den sicheren Zustand (0) versetzt.

Informationen dazu, wie die Befehle der GuardLogix-Sicherheitsanwendung verwendet werden, finden Sie in Anhang F dieses Handbuchs und im Referenzhandbuch „Befehlssatz für GuardLogix-Sicherheitsanwendungen“, Publikation 1756-RM095.

## Befehle „Erhalt des Systemwerts“ (GSV) und „Setzen des Systemwerts“ (SSV)

Mit den Befehlen GSV und SSV können Sie die in den Geräteobjekten gespeicherten Steuerungssystemdaten abrufen (GSV) und festlegen (SSV). Wenn Sie einen GSV/SSV-Befehl eingeben, zeigt die Programmiersoftware die gültigen Objektklassen, Objektnamen und Attributnamen für jeden Befehl an. Es gelten Beschränkungen für die Verwendung der GSV- und SSV-Befehle mit Sicherheitskomponenten.

| | |
|---|---|
| **WICHTIG** | Die Sicherheits-Task kann GSV- oder SSV-Operationen nicht für Standardattribute ausführen.<br>Die Attribute von Sicherheitsobjekten, die von der Standard-Task geschrieben werden können, dienen nur zur Diagnose. Sie haben keinen Einfluss auf die Ausführung der Sicherheits-Task. |

Nähere Informationen dazu, welche Sicherheitsattribute über GSV- und SSV-Befehle zur Verfügung stehen, finden Sie im Benutzerhandbuch „GuardLogix 5570 Controllers User Manual“, Publikation 1756-UM022.

Allgemeine Informationen zur Verwendung von GSV- und SSV-Befehlen finden Sie im Referenzhandbuch „Logix5000 Steuerungen – Allgemeine Befehle“, Publikation 1756-RM003.

## GuardLogix-Systemstörungen

Störungen im GuardLogix-System lassen sich in die folgenden drei Kategorien unterteilen:

- Nicht korrigierbare Steuerungsfehler
- Nicht korrigierbare Sicherheitsfehler
- Korrigierbare Fehler

Informationen zur Handhabung von Fehlern finden Sie im Benutzerhandbuch „GuardLogix 5570 Controllers User Manual", Publikation 1756-UM022.

### Nicht korrigierbare Steuerungsfehler

Ein nicht korrigierbarer Steuerungsfehler tritt auf, wenn die interne Diagnose der Steuerung ausfällt. Die Partnerschaft geht verloren, wenn sich ein nicht korrigierbarer Steuerungsfehler in der Primärsteuerung oder dem Sicherheitspartner ereignet und damit der jeweils andere einen nicht korrigierbaren Fehler mit Timeout des Überwachungszeitraums erzeugt. Die Ausführung der Standard-Task und Sicherheits-Task wird angehalten und die Sicherheits-E/A gehen in den sicheren Zustand über.

Zur Wiederherstellung des Betriebs nach einem nicht korrigierbaren Steuerungsfehler muss das Anwendungsprogramm erneut heruntergeladen werden.

### Nicht korrigierbare Sicherheitsfehler

Bei einem nicht korrigierbaren Sicherheitsfehler protokolliert die Steuerung die Störung in der Fehlerbehandlung im Steuerungsbereich und schaltet die Sicherheits-Task einschließlich Sicherheits-E/A und Sicherheitslogik aus.

Zur Wiederherstellung des Betriebs nach einem nicht korrigierbaren Sicherheitsfehler wird der Sicherheitsspeicher von der Sicherheits-Task-Signatur (geschieht automatisch, wenn Sie die Störung beheben) oder, falls keine Sicherheits-Task-Signatur existiert, über ein explizites Herunterladen des Sicherheitsprojekts neu initialisiert.

Sie können den Sicherheitsfehler überbrücken, indem Sie den Eintrag im Fehlerlog über die Sicherheitsfehlerbehandlung im Steuerungsbereich löschen. Dadurch können Standard-Tasks weiter ausgeführt werden.



**ACHTUNG:** Der Sicherheitsfehler wird durch Überbrücken nicht gelöscht! Wenn Sie den Sicherheitsfehler überbrücken, obliegt es Ihnen zu beweisen, dass dabei weiterhin SIL 3 beibehalten wird.

## Korrigierbare Fehler

Steuerungsfehler, die durch Anwenderprogrammierfehler in einem Sicherheitsprogramm verursacht werden, veranlassen die Steuerung, die in der Fehlerbehandlung des Sicherheitsprogramms des Projekts enthaltene Logik zu verarbeiten. Die Fehlerbehandlung des Sicherheitsprogramms gibt der Anwendung die Möglichkeit, den Fehlerzustand zu beheben und danach den Betrieb wiederherzustellen.



**ACHTUNG:** Sie müssen Ihrer Zertifizierungsstelle den Nachweis erbringen, dass die automatische Wiederherstellung des Betriebs nach korrigierbaren Störungen SIL 3 beibehält.

Wenn keine Fehlerbehandlung des Sicherheitsprogramms existiert oder die Störung von ihr nicht korrigiert wird, verarbeitet die Steuerung die Logik in der Fehlerbehandlung im Steuerungsbereich und beendet damit die Ausführung der Sicherheitsprogrammierlogik und lässt die Sicherheits-E/A-Verbindungen aktiv, aber leer laufend.

**WICHTIG** Wenn die Ausführung der Sicherheitsprogrammierlogik aufgrund eines korrigierbaren Fehlers beendet wird, der nicht von der Fehlerbehandlung des Sicherheitsprogramms gehandhabt wird, werden die Sicherheits-E/A-Verbindungen geschlossen und erneut geöffnet, um die Sicherheitsverbindungen neu zu initialisieren.

Falls Anwenderlogik infolge einer korrigierbaren Störung, die nicht korrigiert wird, beendet wird, werden Sicherheitsausgänge in den sicheren Zustand gesetzt und der Producer der sicherheitsbezogen konsumierten Tags gibt dem Consumer den Befehl, diese in einen sicheren Zustand zu setzen.

**TIPP** Bei Verwendung von Sicherheits-E/A für Standardapplikationen wird Sicherheits-E/A infolge des oben Beschriebenen der Befehl gegeben, in den sicheren Zustand überzugehen.

Falls ein korrigierbarer Sicherheitsfehler in der Fehlerbehandlung im Steuerungsbereich überbrückt wird, werden nur Standard-Tasks weiter ausgeführt. Wird der Fehler nicht überbrückt, werden auch die Standard-Tasks abgeschaltet.



**ACHTUNG:** Der Sicherheitsfehler wird durch Überbrücken nicht gelöscht! Wenn Sie den Sicherheitsfehler überbrücken, obliegt es Ihnen zu beweisen, dass dabei weiterhin SIL 3 beibehalten wird.

# Notizen:

# Sicherheitsbefehle

Die neuesten Informationen finden Sie in unseren Sicherheitszertifikaten unter http://www.rockwellautomation.com/products/certification/safety/.

Tabelle 9 und Tabelle 10 enthalten die Befehle zu den Sicherheitsanwendungen, die für die Verwendung in SIL 3-Anwendungen zertifiziert sind.

**Tabelle 9 – Allgemeine Befehle für Sicherheitsanwendungen**

| Mnemonik | Name | Aufgabe | Zertifizierung |
|---|---|---|---|
| CROUT | Configurable Redundant Output (Konfigurierbarer redundanter Ausgang) | Steuert und überwacht redundante Ausgänge. | • BG<br>• TÜV |
| DCA | Dual Channel Input – Analog (integer version) (Zweikanaleingang – Analog (ganzzahlige Ausführung)) | Überwacht zwei Analogwerte auf Abweichungen und Bereichstoleranz. | TÜV |
| DCAF | Dual Channel Input – Analog (floating point version) (Zweikanaleingang – Analog (Fließkomma-Ausführung)) | | |
| DCS | Dual Channel Input – Stop (Zweikanaleingang – Stopp) | Überwacht mit zwei Eingängen versehene Sicherheitsgeräte, deren Hauptaufgabe darin besteht, eine Stoppfunktion wie z. B. einen Not-Halt, ein Lichtgitter oder einen Gate Switch zur Verfügung zu stellen. | • BG<br>• TÜV |
| DCST | Dual Channel Input – Stop With Test (Zweikanaleingang – Stopp mit Test) | Überwacht mit zwei Eingängen versehene Sicherheitsgeräte, deren Hauptaufgabe darin besteht, eine Stoppfunktion wie z. B. einen Not-Halt, ein Lichtgitter oder einen Gate Switch zur Verfügung zu stellen. Bietet die zusätzliche Fähigkeit, einen Funktionstest des Stoppgeräts zu initialisieren. | • BG<br>• TÜV |
| DCSTL | Dual Channel Input – Stop With Test and Lock (Zweikanaleingang – Stopp mit Test und Verriegelung) | Überwacht mit zwei Eingängen versehene Sicherheitsgeräte, deren Hauptaufgabe darin besteht, eine Stoppfunktion wie z. B. einen Not-Halt, ein Lichtgitter oder einen Gate Switch zur Verfügung zu stellen. Bietet die zusätzliche Fähigkeit, einen Funktionstest des Stoppgeräts zu initialisieren. Kann ein Rückführungssignal von einem Sicherheitsgerät überwachen und eine Sperranforderung an ein Sicherheitsgerät ausgeben. | • BG<br>• TÜV |
| DCSTM | Dual Channel Input – Stop With Test and Mute (Zweikanaleingang – Stopp mit Test und Muting) | Überwacht mit zwei Eingängen versehene Sicherheitsgeräte, deren Hauptaufgabe darin besteht, eine Stoppfunktion wie z. B. einen Not-Halt, ein Lichtgitter oder einen Gate Switch zur Verfügung zu stellen. Bietet zusätzlich die Fähigkeit, einen Funktionstest des Stoppgeräts zu initialisieren und das Sicherheitsgerät temporär zu deaktivieren. | TÜV |
| DCM | Dual Channel Input – Monitor (Zweikanaleingang – Überwachung) | Überwacht mit zwei Eingängen versehene Sicherheitsgeräte. | • BG<br>• TÜV |
| DCSRT | Dual Channel Input – Start (Zweikanaleingang – Start) | Schaltet mit zwei Eingängen versehene Sicherheitsgeräte ein, deren Hauptfunktion darin besteht, eine Maschine sicher zu starten (z. B. Zustimmtaster). | • BG<br>• TÜV |
| SMAT | Safety Mat (Sicherheitsmatte) | Gibt an, ob die Sicherheitsmatte belegt ist. | TÜV |
| THRSe | Two-Hand Run Station – Enhanced (Zweihandbedienstation – erweitert) | Überwacht zwei diversitäre Sicherheitseingänge, einen von einer rechten und einen von einer linken Drucktaste, zur Steuerung eines einzigen Ausgangs. Bietet eine konfigurierbare Kanal-zu-Kanal-Diskrepanzzeit und die erweiterte Fähigkeit, eine Zweihandbedienstation zu überbrücken. | • BG<br>• TÜV |
| TSAM | Two Sensor Asymmetrical Muting (Muting mit zwei Sensoren in asymmetrischer Anordnung) | Deaktiviert die Schutzfunktion eines Lichtgitters mithilfe zweier asymmetrisch angeordneter Muting-Sensoren vorübergehend automatisch. | TÜV |
| TSSM | Two Sensor Symmetrical Muting (Muting mit zwei Sensoren in symmetrischer Anordnung) | Deaktiviert die Schutzfunktion eines Lichtgitters mithilfe zweier symmetrisch angeordneter Muting-Sensoren vorübergehend automatisch. | TÜV |
| FSBM | Four Sensor Bidirectional Muting (Muting mit vier Sensoren in bidirektionaler Anordnung) | Deaktiviert die Schutzfunktion eines Lichtgitters mithilfe von vier Sensoren, die vor und nach dem Abtastungsfeld des Lichtgitters hintereinander angeordnet sind, vorübergehend automatisch. | TÜV |

**Tabelle 10 – Befehle für Sicherheitsanwendungen – Umformverfahren**

| Mnemonik | Name | Aufgabe | Zertifizierung |
|---|---|---|---|
| CBCM | Clutch Brake Continuous Mode (Dauerbetrieb Kupplungsbremse) | Wird für Pressenanwendungen verwendet, in denen ein kontinuierlicher Betrieb erwünscht ist. | • BG<br>• TÜV |
| CBIM | Clutch Brake Inch Mode (Tippbetrieb Kupplungsbremse) | Wird für Pressenanwendungen verwendet, in denen kleine Anpassungen des Pressenstößels erforderlich sind, z. B. die Konfiguration der Presse. | • BG<br>• TÜV |
| CBSSM | Clutch Brake Single Stroke Mode (Einzelhubbetrieb Kupplungsbremse) | Wird in Pressenanwendungen mit Einzelzyklus verwendet. | • BG<br>• TÜV |
| CPM | Crankshaft Position Monitor (Überwachung Kurbelwellenposition) | Dient dazu, die Position des Pressenstößels zu überwachen. | • BG<br>• TÜV |
| CSM | Camshaft Monitor (Überwachung Nockenwelle) | Überwacht die Bewegungen zum Starten, Stoppen und Ausführen des Betriebs einer Nockenwelle. | • BG<br>• TÜV |
| EPMS | Eight-position Mode Selector (8-fach-Betriebsartenwahlschalter) | Überwacht acht Sicherheitseingänge zur Steuerung eines von acht Ausgängen, der dem aktiven Eingang entspricht. | • BG<br>• TÜV |
| AVC | Auxiliary Valve Control (Steuerung Hilfsventil) | Steuert ein Hilfsventil, das zusammen mit einem Hauptventil verwendet wird. | TÜV |
| MVC | Main Valve Control (Steuerung Hauptventil) | Steuert und überwacht ein Hauptventil. | • BG<br>• TÜV |
| MMVC | Maintenance Manual Valve Control (Manuelle Ventilsteuerung bei Wartung) | Dient dazu, ein Ventil während der Instandhaltung manuell zu steuern. | • BG<br>• TÜV |

Routinen in der Sicherheits-Task können diese Kontaktplanlogik-Sicherheitsbefehle verwenden.

**Tabelle 11 – Kontaktplanlogik-Sicherheitsbefehle**

| Typ | Mnemonik | Name | Aufgabe |
|---|---|---|---|
| Datenfeld (Datei) | FAL(1) | File Arithmetic and Logic (Dateiarithmetik und Logik) | Kopier-, Arithmetik-, Logik- und Funktionsvorgänge zu den in einem Datenfeld gespeicherten Daten durchführen |
| | FLL(1) | File Fill (Datei füllen) | Element eines Datenfelds mit dem Ausgangswert (Datentyp) füllen, wobei der Ausgangswert (Datentyp) unverändert bleibt |
| | FSC(1) | File Search and Compare (Datei suchen und vergleichen) | Wert in einem Datenfeld elementweise vergleichen |
| | SIZE(1) | Size In Elements (Größe in Elementen) | Größe der Dimension eines Datenfelds finden |
| Bit | XIC | Examine If Closed (Auf geschlossen prüfen) | Auf geschlossen prüfen – Ausgänge aktivieren, wenn ein Bit eingerichtet wurde |
| | XIO | Examine If Open (Auf offen prüfen) | Auf offen prüfen – Ausgänge aktivieren, wenn ein Bit gelöscht wurde |
| | OTE | Output Energize (Ausgang einschalten) | Ausgang einschalten – Bit einrichten |
| | OTL | Output Latch (Ausgang verriegeln) | Ausgang verriegeln – Bit einrichten (remanent) |
| | OTU | Output Unlatch (Ausgang entriegeln) | Ausgang entriegeln – Bit löschen (remanent) |
| | ONS | One Shot (Einzelimpuls) | Einzelimpuls – einmal durchzuführendes Ereignis auslösen |
| | OSR | One Shot Rising (Steigender Einzelimpuls) | Steigender Einzelimpuls – an der (steigenden) False-nach-True-Flanke der Zustandsänderung einmal durchzuführendes Ereignis |
| | OSF | One Shot Falling (Fallender Einzelimpuls) | Fallender Einzelimpuls – an der (fallenden) True-nach-False-Flanke der Zustandsänderung einmal durchzuführendes Ereignis |

**Tabelle 11 – Kontaktplanlogik-Sicherheitsbefehle**

| Typ | Mnemonik | Name | Aufgabe |
|---|---|---|---|
| Zeitwerk | TON | Timer On Delay (Timer-Einschaltverzögerung) | Timer-Einschaltverzögerung – Einrichten, wie lange ein Zeitwerk aktiviert ist |
| | TOF | Timer Off Delay (Timer-Ausschaltverzögerung) | Timer-Ausschaltverzögerung – Einrichten, wie lange ein Zeitwerk deaktiviert ist |
| | RTO | Retentive Timer On (Speichernder Timer EIN) | Speichernder Timer EIN – Zeit akkumulieren |
| | CTU | Count Up (Aufwärtszählung) | Aufwärtszählung |
| | CTD | Count Down (Abwärtszählung) | Abwärtszählung |
| | RES | Reset (Rücksetzen) | Rücksetzen – Zeitwerk oder Zähler zurücksetzen |
| Vergleichen | CMP(1)(2) | Compare (Vergleichen) | Vergleich zu den Rechenoperationen durchführen, die Sie im Ausdruck angegeben haben |
| | EQU | Equal To (Gleich) | Gleich – Testen, ob zwei Werte gleich sind |
| | GEQ | Greater Than Or Equal To (Größer als oder gleich) | Größer als oder gleich – Prüfen, ob ein Wert größer als ein anderer oder gleich einem anderen Wert ist |
| | GRT | Greater Than (Größer als) | Größer als – Prüfen, ob ein Wert größer als ein anderer Wert ist |
| | LEQ | Less Than Or Equal To (Kleiner als oder gleich) | Kleiner als oder gleich – Prüfen, ob ein Wert kleiner als ein anderer oder gleich einem anderen Wert ist |
| | LES | Less Than (Kleiner als) | Kleiner als – Prüfen, ob ein Wert kleiner als ein anderer Wert ist |
| | MEQ | Masked Comparison for Equal (Maskierter Vergleich auf gleich) | Maskierter Vergleich auf gleich – Ausgangs- und Vergleichswerte durch eine Maske leiten und prüfen, ob sie gleich sind |
| | NEQ | Not Equal To (Ungleich) | Ungleich – Prüfen, ob ein Wert nicht gleich einem anderen Wert ist |
| | LIM | Limit Test (Grenzwerttest) | Grenzwerttest – Prüfen, ob ein Wert innerhalb eines bestimmten Bereichs liegt |
| Bewegen | CLR | Clear (Löschen) | Löschen – Wert löschen |
| | COP(3) | Copy (Kopieren) | Kopieren – Wert kopieren |
| | MOV | Move (Bewegen) | Kopieren – Wert kopieren |
| | MVM | Masked Move (Maskierte Verschiebung) | Maskierte Verschiebung – Bestimmten Teil einer Ganzzahl kopieren |
| | SWPB(1) | Swap Byte (Byte tauschen) | Byte eines Werts neu anordnen |
| Logisch | AND | Bitwise AND (Logische Und-Operation) | Logische Und-Operation – Bitweise UND-Vorgänge durchführen |
| | NOT | Bitwise NOT (Logisches Nicht) | Logisches Nicht – Bitweise NICHT-Vorgänge durchführen |
| | OR | Bitwise OR (Logisches Oder) | Logisches Oder – Bitweise ODER-Vorgänge durchführen |
| | XOR | Bitwise Exclusive OR (Exklusives Oder) | Exklusives Oder – Bitweise exklusive ODER-Vorgänge durchführen |
| Programm-steuerung | JMP | Jump To Label (Sprung) | Sprung – Logikabschnitt überspringen, der nicht immer ausgeführt werden muss (springt zum darauf verweisenden LBL-Befehl) |
| | LBL | Label (Marke) | Marke – Kennzeichnen eines Befehls, sodass über einen JMP-Befehl auf diesen verwiesen werden kann |
| | JSR | Jump to Subroutine (Sprung ins Unterprogramm) | Sprung ins Unterprogramm – Zu separater Routine springen |
| | RET | Return (Rückkehr vom Unterprogramm) | Rückkehr vom Unterprogramm – Ergebnisse eines Unterprogramms zurückgeben |
| | SBR | Subroutine (Unterprogramm) | Unterprogramm – Daten an ein Unterprogramm senden |
| | TND | Temporary End (Temporäres Ende) | Temporäres Ende – Kennzeichnung, die die Ausführung einer Routine unterbricht |
| | MCR | Master Control Reset (Hauptsteuerbefehl) | Jeden Strompfad in einem Logikabschnitt deaktivieren |
| | AFI | Always False Instruction (Immer unwahr) | Immer unwahr – Strompfad deaktivieren |
| | NOP | No Operation (Kein Betrieb) | Kein Betrieb – Platzhalter in Logik einfügen |
| | EVENT | Trigger Event Task (Ereignis-Task auslösen) | Eine Ausführung einer Ereignis-Task auslösen(5) |

**Tabelle 11 – Kontaktplanlogik-Sicherheitsbefehle**

| Typ | Mnemonik | Name | Aufgabe |
|---|---|---|---|
| Berechnen | Add (Addition) | Add (Addition) | Addition – Zwei Werte addieren |
| | CPT(1) | Compute (Berechnen) | Die im Ausdruck definierte Rechenoperation durchführen |
| | SUB | Subtract (Subtraktion) | Subtraktion – Zwei Werte subtrahieren |
| | MUL | Multiply (Multiplikation) | Multiplikation – Zwei Werte multiplizieren |
| | DIV | Divide (Division) | Division – Zwei Werte teilen |
| | MOD | Modulo | Restwert bestimmen, nachdem ein Wert durch einen anderen Wert geteilt wurde |
| | SQR | Square Root (Quadratwurzel) | Quadratwurzel eines Werts berechnen |
| | NEG | Negate (Negation) | Negation – Entgegengesetztes Zeichen eines Werts annehmen |
| | ABS | Absolute Value (Absolutwert) | Absolutwert – Absoluten Wert eines Werts annehmen |
| E/A | GSV(4) | Get System Value (Erhalt des Systemwerts) | Erhalt des Systemwerts – Informationen zum Steuerungsstatus abrufen |
| | SSV(4) | Set System Value (Setzen des Systemwerts) | Setzen des Systemwerts – Informationen zum Steuerungsstatus einrichten |

(1) Nur auf den Steuerungen 1756-L7*x*S und 1756-L7*x*SXT unterstützt. Für den Datentyp REAL wird auf den Steuerungen 1756-L7*x*S und 1756-L7*x*SXT ein Fließkommaformat für Sicherheitsroutinen unterstützt.

(2) Erweiterte Operanden wie SIN, COS und TAN werden in Sicherheitsroutinen nicht unterstützt.

(3) Der Längenoperand muss eine Konstante sein, wenn der COP-Befehl in einer Sicherheitsroutine verwendet wird. Die Längen von Quelle und Ziel müssen identisch sein.

(4) Besondere Hinweise zur Verwendung der GSV- und SSV-Befehle finden Sie in der Publikation 1756-UM022, „GuardLogix 5570-Steuerungen – Benutzerhandbuch".

(5) Der Ereignisbefehl löst einen Scan der Standard-Task aus.

**WICHTIG** Wenn Sie direkte Achssteuerungsbefehle mit einem Kinetix 5500-Servoantrieb verwenden, finden Sie im Benutzerhandbuch „Kinetix 5500-Servoantriebe", Publikation 2198-UM001, Informationen zur Verwendung dieser Funktion in Sicherheitsanwendungen.

Weitere Informationen finden Sie in den folgenden Publikationen.

**Tabelle 12 – Weitere Informationsquellen**

| Quelle | Beschreibung |
|---|---|
| Referenzhandbuch „Befehlssatz für GuardLogix-Sicherheitsanwendungen", Publikation 1756-RM095 | Enthält Informationen zu den Befehlen für die Sicherheitsanwendung |
| Referenzhandbuch „Logix5000-Steuerungen – Allgemeine Befehle", Publikation 1756-RM003 | Enthält detaillierte Informationen zum Logix-Befehlssatz |

# Sicherheits-Add-On-Befehle



Mit der Anwendung Logix Designer können Sie Sicherheits-Add-On-Befehle erzeugen. Sicherheits-Add-On-Befehle ermöglichen es Ihnen, häufig verwendete Sicherheitslogik zu einem einzigen Befehl zusammenzufassen, wodurch sie modular und dadurch einfacher zu verwenden ist.

Sicherheits-Add-On-Befehle verwenden die Befehlssignatur von Add-On-Befehlen hoher Integrität sowie eine SIL 3-Sicherheitsbefehlssignatur zur Verwendung in sicherheitstechnischen Funktionen bis einschließlich SIL 3.

## Erstellen und Verwenden eines Sicherheits-Add-On-Befehls

In dem Flussdiagramm auf Seite 74 sind die Schritte aufgeführt, die erforderlich sind, um einen Sicherheits-Add-On-Befehl zu erstellen und anschließend in einem SIL 3-Sicherheitsanwendungsprogramm zu verwenden. Bei den schattierten Elementen handelt es sich um Schritte, die ausschließlich für Add-On-Befehle gelten. Die Elemente in Fettdruck werden auf den Seiten erläutert, die sich an das Flussdiagramm anschließen.

**Abbildung 18 – Flussdiagramm zur Erstellung und Verwendung von Sicherheits-Add-On-Befehlen**

Zum Erstellen eines Sicherheits-Add-On-Befehls

**Add-On-Befehl-Testprojekt erstellen**

**Sicherheits-Add-On-Befehl erstellen**

**Befehlssignatur erzeugen**

Testprogramm erstellen/ändern

Herunterladen **(Sicherheitsbefehlssignatur erzeugen)**

In Run-Modus wechseln

**SIL 3-Qualifizierungstest zu Add-On-Befehlen durchführen**

Alle Tests bestanden?

Nein

Ja

**Projekt bestätigen**

**Add-On-Befehl einer Sicherheitsvalidierung unterziehen**

**Eintrag in Signatur-History erstellen (offline)**

Befehlssignatur, Datum/Uhrzeit und Sicherheitsbefehlssignatur aufzeichnen

**Sicherheits-Add-On-Befehl exportieren**

Sicherheits-Add-On-Befehl steht zur Verwendung zur Verfügung

Zum Ändern eines Sicherheits-Add-On-Befehls (offline)

Sicherheits-Add-On-Befehl ändern

Befehlssignatur löschen

Offline gehen

Sicherheits-Task-Signatur löschen, sofern vorhanden

Zum Verwenden eines Sicherheits-Add-On-Befehls

Projekt erstellen oder öffnen

**Sicherheits-Add-On-Befehl importieren**

Anwendung erstellen/ändern

Herunterladen

**Signaturen des Sicherheits-Add-On-Befehls verifizieren**

Befehlssignatur gültig?

Nein

Zurück zum ursprünglichen Testprojekt

Ja

Sicherheitsbefehlssignatur gültig?

Nein

Zurück zum ursprünglichen Testprojekt

Ja

**Anwendungsprogramm testen**

In Programm-Modus wechseln

Sicherheits-Task-Signatur erstellen

**Projekt bestätigen**

In Run-Modus wechseln

**Projektverifizierungstest**

Alle Tests bestanden?

Nein

Sind Änderungen am Add-On-Befehl erforderlich?

Nein

Sicherheits-Task-Signatur löschen

Erforderliche Änderungen vornehmen

Ja

Ja

Sicherheits-Task-Signatur aufzeichnen

**Projekt einer Sicherheitsvalidierung unterziehen**

Projekt gültig?

Nein

Ja

Fertig

## Add-On-Befehl-Testprojekt erstellen

Sie müssen eigens zum Erstellen und Testen des Sicherheits-Add-On-Befehls ein eindeutiges Textprojekt erstellen. Bei diesem Projekt muss es sich um ein separates und eigenes Projekt handeln, damit unerwartete Einflüsse minimiert werden.

Befolgen Sie die Leitlinien für Projekte im Kapitel Projekt erstellen auf Seite 53.

## Sicherheits-Add-On-Befehl erstellen

Eine Anleitung zum Erstellen von Add-On-Befehlen finden Sie im Programmierhandbuch zu Add-On-Befehlen für Logix5000-Steuerungen („Logix5000 Controllers Add-On Instructions“), Publikation 1756-PM010.

## Befehlssignatur erzeugen

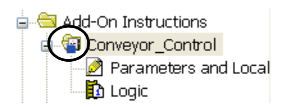
Anhand der Befehlssignatur können Sie schnell feststellen, ob der Befehl geändert wurde. Jeder Add-On-Befehl kann über eine eigene Signatur verfügen. Diese Befehlssignatur ist erforderlich, wenn ein Add-On-Befehl in sicherheitstechnischen Funktionen verwendet wird. Ebenso kann sie manchmal auch in den regulierten Industriebranchen erforderlich werden. Verwenden Sie sie, wenn Ihre Anwendung einen höheren Grad an Integrität erfordert.

Die Befehlssignatur besteht aus einer ID-Nummer und einem Zeitstempel, der den Inhalt des Add-On-Befehls zu einem bestimmten Zeitpunkt identifiziert.

Einmal erzeugt, versiegelt die Befehlssignatur den Add-On-Befehl sozusagen und verhindert so, dass der Befehl bearbeitet werden kann, während die Signatur vorliegt. Diese Einschränkung schließt auch Strompfadkommentar, Tag-Beschreibungen und jede andere Befehlsdokumentation ein, die erstellt wurde. Wenn der Befehl versiegelt wurde, können Sie nur folgende Aktionen durchführen:

- Befehlssignatur kopieren
- Eintrag in Signatur-History erstellen oder kopieren
- Instanzen des Add-On-Befehls erstellen
- Befehl herunterladen
- Befehlssignatur entfernen
- Berichte ausdrucken

Wurde eine Befehlssignatur erzeugt, dann zeigt die Anwendung Logix Designer die Befehlsdefinition mit dem Symbol des Siegels an.




| WICHTIG | Falls Sie vorhaben, Ihren Add-On-Befehl mithilfe der in der Anwendung Logix Designer enthaltenen Schutzfunktion für Quellen zu schützen, dann müssen Sie den Quellenschutz vor dem Erzeugen der Befehlssignatur aktivieren. |
|---|---|

## Sicherheitsbefehlssignatur herunterladen und erzeugen

Wenn ein versiegelter Sicherheits-Add-On-Befehl zum ersten Mal heruntergeladen wird, dann wird automatisch eine SIL 3-Sicherheitsbefehlssignatur erzeugt. Bei der Sicherheitsbefehlssignatur handelt es sich um eine ID-Nummer, die die Ausführungsmerkmale des Sicherheits-Add-On-Befehls identifiziert.

## SIL 3-Qualifizierungstest zu Add-On-Befehlen

SIL 3-Tests zu Sicherheits-Add-On-Befehlen müssen in einer separaten, eigenen Anwendung durchgeführt werden, um sicherzustellen, dass unerwünschte Einflüsse minimiert werden. Sie müssen einen gut ausgearbeiteten Testplan befolgen und einen Einheitentest des Sicherheits-Add-On-Befehls durchführen, bei dem alle möglichen Ausführungspfade durch die Logik sowie die gültigen und ungültigen Bereiche aller Eingangsparameter ausgeführt werden.

Die Entwicklung aller Sicherheits-Add-On-Befehle hat gemäß IEC 61508 – „Requirements for software module testing“ zu erfolgen. Diese Norm enthält detaillierte Anforderungen, die an den Einheitentest gestellt werden.

## Projekt bestätigen

Sie müssen das Projekt ausdrucken oder anzeigen und die hochgeladenen Sicherheits-E/A- und Steuerungskonfigurationen, Sicherheitsdaten, Sicherheits-Add-On-Befehle sowie die Programmlogik der Sicherheits-Task manuell vergleichen, um sicherzustellen, dass die richtigen Sicherheitskomponenten heruntergeladen, getestet und im Sicherheitsanwendungsprogramm gespeichert wurden.

Unter Projekt bestätigen auf Seite 55 wird beschrieben, wie Sie ein Projekt bestätigen können.

## Add-On-Befehle einer Sicherheitsvalidierung unterziehen

Eine unabhängige Überprüfung des Sicherheits-Add-On-Befehls durch einen Dritten ist ggf. erforderlich, bevor der Befehl zur Verwendung freigegeben wird. Eine unabhängige Validierung durch einen Dritten ist für IEC 61508 SIL 3 erforderlich.

## Eintrag in der Signatur-History erstellen

Mit der Signatur-History steht ein Datensatz zur Verfügung, der später als Referenz verwendet werden kann. Der Eintrag in der Signatur-History besteht aus der Befehlssignatur, dem Namen des Benutzers, dem Wert des Zeitstempels und einer benutzerdefinierten Beschreibung. Es können bis zu sechs History-Einträge gespeichert werden. Um einen Eintrag in der Signatur-History zu erstellen, müssen Sie offline sein.

**TIPP** Über den Bericht „Signature Listing" (Signaturliste) in der Anwendung Logix Designer werden Befehlssignatur, Zeitstempel und Sicherheitsbefehlssignatur ausgedruckt. Um den Bericht auszudrucken, klicken Sie im Controller Organizer mit der rechten Maustaste auf „Add-On Instruction" und dann auf „Print > Signature Listing".

## Sicherheits-Add-On-Befehl exportieren und importieren

Wenn Sie einen Sicherheits-Add-On-Befehl exportieren, wählen Sie die Option, um alle referenzierten Add-On-Befehle und benutzerdefinierten Typen (User-Defined Types) in dieselbe Exportdatei einzuschließen. Wenn Sie die referenzierten Add-On-Befehle einschließen, wird es einfacher, die Signaturen zu erhalten.

Beachten Sie beim Importieren von Add-On-Befehlen bitte folgende Leitlinien:

- Sie können keinen Sicherheits-Add-On-Befehl in ein Standardprojekt importieren.
- Sie können keinen Sicherheits-Add-On-Befehl in ein Sicherheitsprojekt importieren, das sicherheitsverriegelt wurde oder über eine Sicherheits-Task-Signatur verfügt.
- Sie können keinen Sicherheits-Add-On-Befehl importieren, während Sie online sind.
- Wenn Sie einen Add-On-Befehl mit einer Befehlssignatur in ein Projekt importieren, in dem keine referenzierten Add-On-Befehle oder benutzerdefinierten Typen zur Verfügung stehen, dann müssen Sie die Signatur möglicherweise entfernen.

### Signaturen des Sicherheits-Add-On-Befehls verifizieren

Nachdem Sie das Anwendungsprojekt mit dem importierten Sicherheits-Add-On-Befehl heruntergeladen haben, müssen Sie die Werte von Befehlssignatur, Datum, Zeitstempel und Sicherheitsbefehlssignatur mit den Originalwerten vergleichen, die Sie vor dem Export des Sicherheits-Add-On-Befehls aufgezeichnet haben. Stimmen sie überein, dann ist der Sicherheits-Add-On-Befehl gültig und Sie können mit der Validierung Ihrer Anwendung fortfahren.

### Anwendungsprogramm testen

Dieser Schritt besteht aus einer Kombination aus Run- und Programm-Modus, Online- oder Offline-Programmbearbeitungen, Hochladen und Herunterladen sowie informellem Testen, das erforderlich ist, um die korrekte Ausführung einer Anwendung zu erreichen.

### Projektverifizierungstest

Führen Sie einen Engineering-Test der Anwendung inklusive Sicherheitssystem durch.

Weitere Informationen finden Sie unter Projektverifizierungstest auf Seite 54.

### Projekt einer Sicherheitsvalidierung unterziehen

Eine unabhängige Überprüfung des Sicherheitssystems durch einen Dritten ist ggf. erforderlich, bevor das System zum Betrieb freigegeben wird. Eine unabhängige Validierung durch einen Dritten ist für IEC 61508 SIL 3 erforderlich.

## Weitere Informationsquellen

Nähere Informationen zur Verwendung von Add-On-Befehlen können Sie folgenden Publikationen entnehmen.

| Quelle | Beschreibung |
|---|---|
| Logix5000 Controllers Add-On Instructions Programming Manual, Publikation 1756-PM010 | Enthält Informationen zu Planung, Erstellung, Verwendung, Import und Export von Add-On-Befehlen in RSLogix 5000-Anwendungen |
| Import/Export Project Components Programming Manual, Publikation 1756-PM019 | Enthält detaillierte Informationen zum Importieren und Exportieren von Projektkomponenten |

# Reaktionszeiten

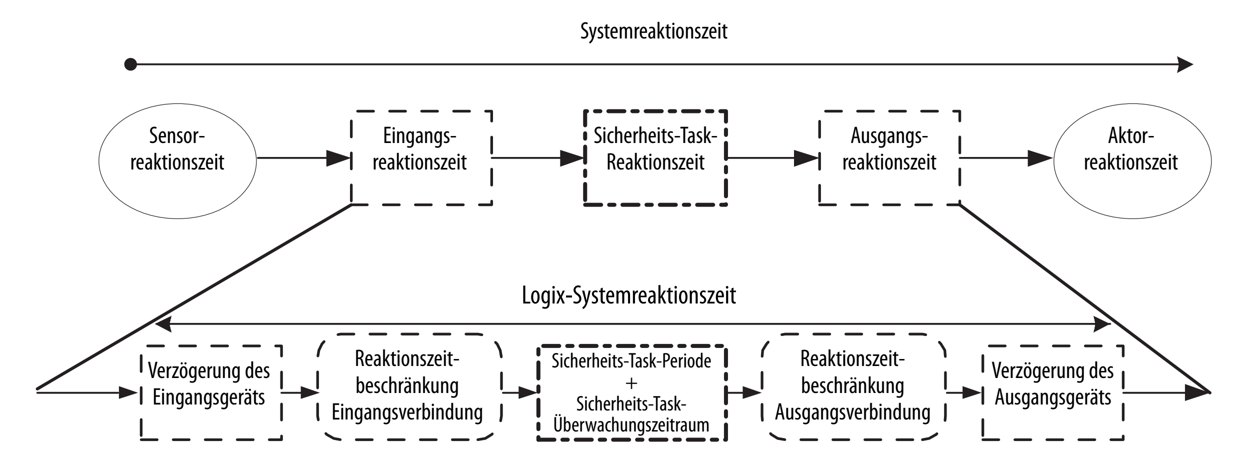


## Systemreaktionszeit

Um die Systemreaktionszeit einer Steuerungskette zu bestimmen, müssen die Reaktionszeiten aller Komponenten der Sicherheitskette addiert werden.

Systemreaktionszeit = Sensorreaktionszeit + Logix-Systemreaktionszeit + Aktorreaktionszeit

**Abbildung 19 – Systemreaktionszeit**

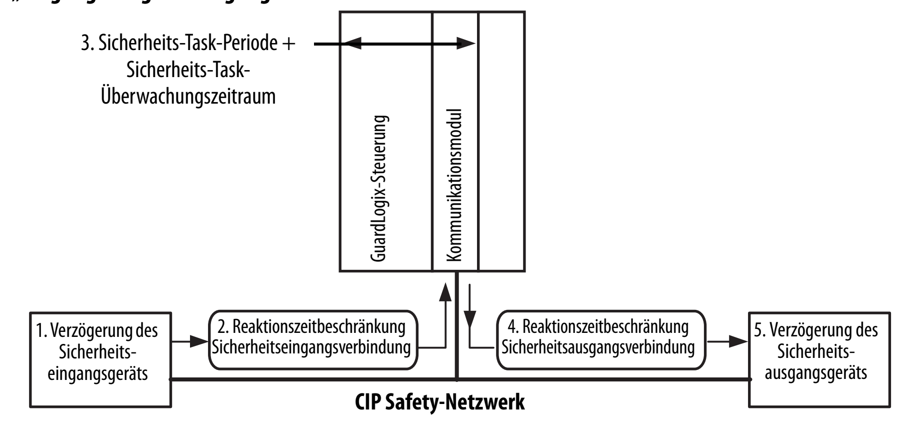



## Logix-Systemreaktionszeit

In den folgenden Abschnitten finden Sie Informationen zur Berechnung der Logix-Systemreaktionszeit für eine einfache Eingang-Logik-Ausgang-Kette sowie für eine komplexere Anwendung, bei der in der Logikkette produzierte/konsumierte Sicherheits-Tags verwendet werden.

## Einfache Kette „Eingang – Logik – Ausgang“

**Abbildung 20 – Längstmögliche Logix-Systemreaktionszeit für eine einfache Kette „Eingang – Logik – Ausgang“**



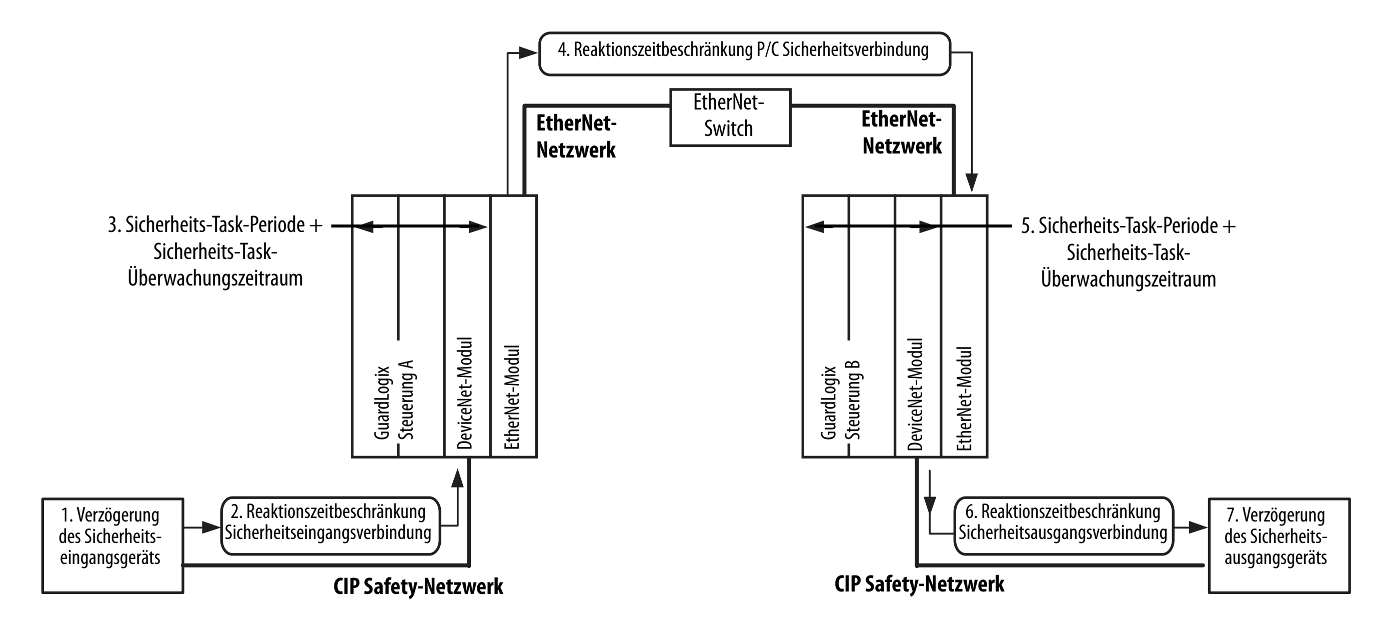

Die Logix-Systemreaktionszeit für jede einfache Eingang-Logik-Ausgang-Kette besteht aus den folgenden fünf Komponenten:

1. Reaktionszeit des Sicherheitseingangsgeräts
(plus Eingangsverzögerungszeit, sofern zutreffend)
2. Reaktionszeitbeschränkung der Sicherheitseingangsverbindung
(Dieser Wert wird in der Anwendung Logix Designer im Dialogfeld „Module Properties“ (Moduleigenschaften) ausgelesen und ist ein Mehrfaches des von der Sicherheitseingangsgerät-Verbindung angeforderten Paketintervalls (RPI).)
3. Sicherheits-Task-Periode plus Sicherheits-Task-Überwachungszeitraum
4. Reaktionszeitbeschränkung Sicherheitsausgangsverbindung
(Dieser Wert wird in der Anwendung Logix Designer im Dialogfeld „Module Properties“ (Moduleigenschaften) ausgelesen und ist ein Mehrfaches der Sicherheits-Task-Periode.)
5. Reaktionszeit des Sicherheitsausgangsgeräts

Zur erleichterten Bestimmung der Reaktionszeit Ihres spezifischen Regelkreises steht im Ordner „Tools“ auf der DVD mit der Studio 5000-Umgebung eine Microsoft Excel-Kalkulationstabelle zur Verfügung.

## Logikkette mit produzierten/konsumierten Sicherheits-Tags

**Abbildung 21 – Logix-Systemreaktionszeit für die Kette „Eingang – Steuerung-A-Logik – Steuerung-B-Logik – Ausgang“**




Die Logix-Systemreaktionszeit für die Kette „Eingang – Steuerung-A-Logik – Steuerung-B-Logik – Ausgang“ besteht aus den folgenden sieben Komponenten:

1. Reaktionszeit des Sicherheitseingangsgeräts (plus Eingangsverzögerungszeit, sofern zutreffend)
2. Reaktionszeitbeschränkung Sicherheitseingangsverbindung
3. Sicherheits-Task-Periode plus Sicherheits-Task-Überwachungszeitraum für Steuerung A
4. Reaktionszeitbeschränkung produzierte/konsumierte Sicherheitsverbindung
5. Sicherheits-Task-Periode plus Sicherheits-Task-Überwachungszeitraum für Steuerung B
6. Reaktionszeitbeschränkung Sicherheitsausgangsverbindung
7. Reaktionszeit des Sicherheitsausgangsgeräts

Zur erleichterten Bestimmung der Reaktionszeit Ihres spezifischen Regelkreises steht im Ordner „Tools“ auf der DVD mit der Studio 5000-Umgebung eine Microsoft Excel-Kalkulationstabelle zur Verfügung.

## Faktoren, die die Komponenten der Logix-Systemreaktionszeit beeinflussen

Die in den vorherigen Abschnitten erläuterten Komponenten der Logix-Reaktionszeiten werden von einer Reihe von Faktoren beeinflusst, die in der folgenden Tabelle beschrieben werden.

**Tabelle 13 – Faktoren, die die Logix-Systemreaktionszeit beeinflussen**

| Komponente der Reaktionszeit | Beeinflussende Faktoren |
|---|---|
| Verzögerung des Eingangsgeräts | Reaktionszeit des Eingangsgeräts |
| | Einstellungen für Ein-Aus und Aus-Ein des jeweiligen Eingangskanals, sofern verfügbar |
| Reaktionszeitbeschränkung Sicherheitseingangsverbindung | Einstellungen des Eingangsgeräts für:<br>• Requested Packet Interval (RPI)<br>• Timeout-Multiplikator<br>• Verzögerungsmultiplikator |
| | Menge des Datenverkehrs im Netzwerk |
| | EMV-Umgebung des Systems |
| Sicherheits-Task-Periode und Sicherheits-Task-Überwachungszeitraum | Einstellung des Zeitraums der Sicherheits-Task |
| | Einstellung des Überwachungszeitraums der Sicherheits-Task |
| | Anzahl und Ausführungszeit der Befehle in der Sicherheits-Task |
| | Tasks mit höherer Priorität, die vor der Sicherheits-Task ausgeführt werden |
| Reaktionszeitbeschränkung produzierte/konsumierte Sicherheitsverbindung | Einstellungen für konsumierte Tags für:<br>• RPI<br>• Timeout-Multiplikator<br>• Verzögerungsmultiplikator |
| | Menge des Datenverkehrs im Netzwerk |
| | EMV-Umgebung des Systems |
| Reaktionszeitbeschränkung Ausgangsverbindung | Einstellung des Zeitraums der Sicherheits-Task |
| | Einstellungen des Ausgangsgeräts für:<br>• Timeout-Multiplikator<br>• Verzögerungsmultiplikator |
| | Menge des Datenverkehrs im Netzwerk |
| | EMV-Umgebung des Systems |
| Verzögerung Ausgangsmodul | Reaktionszeit Ausgangsmodul |

Die folgenden Abschnitte erläutern, wie Sie auf die Daten oder Einstellungen für viele dieser Faktoren zugreifen.

### Zugriff auf die Einstellungen für die Verzögerungszeit des Guard I/O-Eingangsmoduls

Gehen Sie wie im Folgenden beschrieben vor, um in der Anwendung Logix Designer die Verzögerungszeit für das Eingangsmodul zu konfigurieren.

1. Klicken Sie in der Baumstruktur mit der rechten Maustaste auf das gewünschte Guard I/O-Modul, und wählen Sie „Properties“ (Eigenschaften) aus.
2. Klicken Sie auf die Registerkarte „Input Configuration“ (Eingangskonfiguration).

3. Stellen Sie die Eingangsverzögerungszeit so ein, wie Sie sie für Ihre Anwendung benötigen.

Module Properties: Enet_Safety (1791ES-IB8XOBV4 1.1)

Safety | Module Info | Internet Protocol | Port Configuration | Input Configuration | Test Output | Output Configuration

| Point | Point Operation: Type | Point Operation: Discrepancy Time (ms) | Point Mode | Test Source | Input Delay Time (ms): Off->On | Input Delay Time (ms): On->Off |
|---|---|---|---|---|---|---|
| 0 | Equivalent | 10 | Safety | None | 0 | 0 |
| 1 | | | Safety | None | 0 | 0 |
| 2 | Single | 0 | Not Used | None | 0 | 0 |
| 3 | | | Not Used | None | 0 | 0 |
| 4 | Single | 0 | Not Used | None | 0 | 0 |
| 5 | | | Not Used | None | 0 | 0 |
| 6 | Single | 0 | Not Used | None | 0 | 0 |
| 7 | | | Not Used | None | 0 | 0 |

Input Error Latch Time: 1000 ms

Status: Offline OK Cancel Apply Help

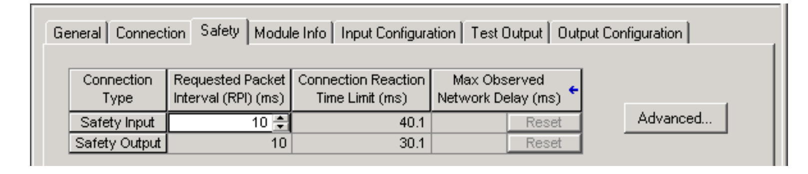
## Zugriff auf die Reaktionszeitbeschränkungen der Eingangs- und Ausgangssicherheitsverbindung

Die Reaktionszeitbeschränkung der Verbindung wird durch die folgenden drei Werte definiert:

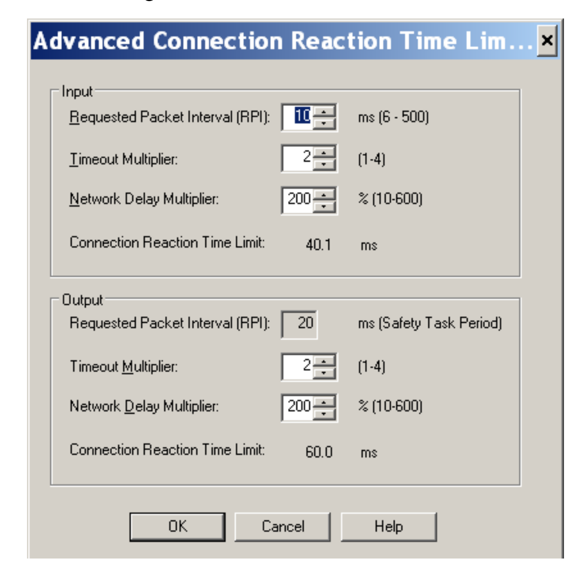
| Wert | Beschreibung |
|---|---|
| Requested Packet Interval (RPI) | Legt fest, wie oft die Eingangs- und Ausgangspakete ins Netzwerk gesendet werden. |
| Timeout-Multiplikator | Beim Timeout-Multiplikator handelt es sich im Wesentlichen um die Zahl der Wiederholungsversuche, bevor es zu einem Timeout kommt. |
| Network Delay Multiplier (Netzwerk-Verzögerungs-multiplikator) | Der Netzwerk-Verzögerungsmultiplikator wird bei bekannten Verzögerungen im Netzwerk eingesetzt. Wenn diese Verzögerungen eintreten, können Timeouts mithilfe dieses Parameters verhindert werden. |

Durch Anpassen dieser Werte können Sie die Reaktionszeitbeschränkung der Verbindung festlegen. Gehen Sie wie folgt vor, um diese Einstellungen anzuzeigen oder zu konfigurieren.

1. Klicken Sie in der Baumstruktur mit der rechten Maustaste auf das gewünschte Sicherheits-E/A-Gerät, und wählen Sie „Properties“ (Eigenschaften) aus.
2. Klicken Sie auf die Registerkarte „Safety“ (Sicherheit).



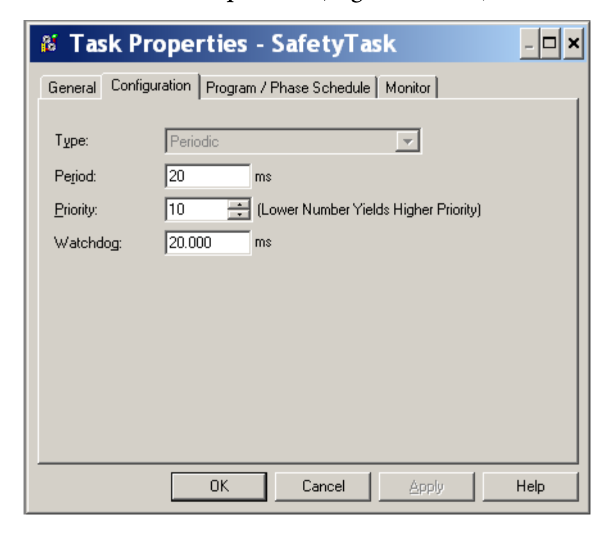
3. Klicken Sie auf „Advanced“ (Erweitert), um das Dialogfeld „Advanced Connection Reaction Time Limit“ (Erweiterte Reaktionszeitbeschränkung der Verbindung) zu öffnen.




## Konfigurieren der Sicherheits-Task-Periode und des Überwachungszeitraums

Die Sicherheits-Task ist eine periodische, d. h. zeitgesteuerte Task. Sie wählen die Task-Priorität („Priority“) und den Überwachungszeitraum („Watchdog“) über das Dialogfeld „Task Properties – Safety Task“ (Task-Eigenschaften – Sicherheits-Task) in Ihrem Logix Designer-Projekt aus.

Um die Einstellungen für die Sicherheits-Task-Periode und den Überwachungszeitraum aufzurufen, klicken Sie mit der rechten Maustaste auf die Sicherheits-Task und wählen dann „Properties“ (Eigenschaften).

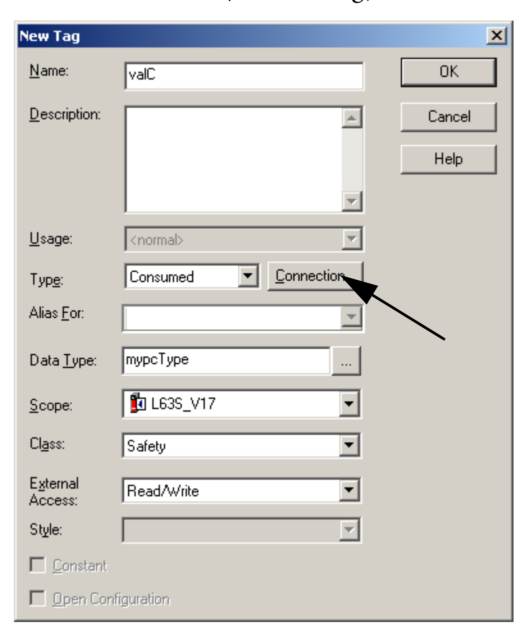



Die Priorität der Sicherheits-Task stellt kein Sicherheitsproblem dar, da der Sicherheits-Task-Überwachungszeitraum überwacht, ob die Task durch eine Task mit höherer Priorität unterbrochen wird.

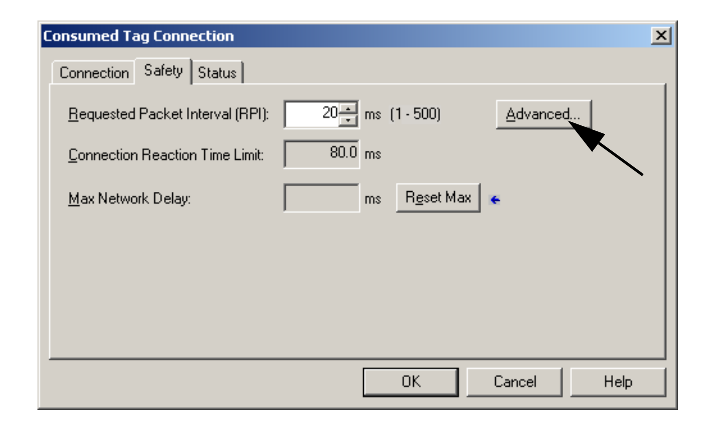
## Zugriff auf produzierte/konsumierte Tag-Daten

Gehen Sie wie folgt vor, um die Verbindungsdaten der Sicherheits-Tags anzuzeigen oder zu konfigurieren.

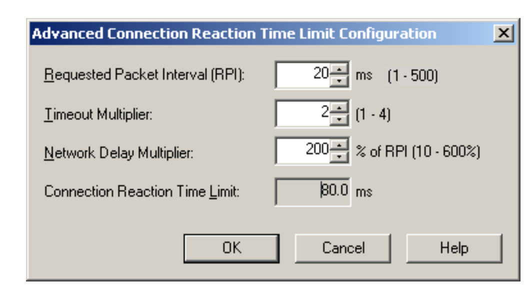
1. Klicken Sie in der Baumkonfiguration mit der rechten Maustaste auf „Controller Tags" (Steuerungs-Tags) und wählen Sie „Edit tags" (Tags bearbeiten).
2. Klicken Sie im Tag Editor mit der rechten Maustaste auf den Namen des Tags, und wählen Sie „Edit Properties" (Eigenschaften bearbeiten).
3. Klicken Sie auf „Connection" (Verbindung).




4. Klicken Sie auf die Registerkarte „Safety" (Sicherheit).



5. Klicken Sie auf „Advanced“ (Erweitert), um die aktuellen Einstellungen anzuzeigen oder zu bearbeiten.




Nähere Informationen hierzu finden Sie in der Publikation 1756-UM022, „GuardLogix 5570-Steuerungen – Benutzerhandbuch“.

# Checklisten für GuardLogix-Sicherheitsanwendungen



Die Checklisten in diesem Anhang sind erforderlich, damit eine SIL 3-zertifizierte GuardLogix-Anwendung geplant, programmiert und gestartet werden kann. Sie können sowohl als Leitlinien für die Planung als auch während der Projektverifizierungstests verwendet werden. Bei der Verwendung als Leitlinien können die Checklisten als Datensätze für den Plan gespeichert werden.

Die Checklisten auf den folgenden Seiten sind als Beispiel für Sicherheitsbetrachtungen zu verstehen und stellen keine vollständige Liste der zu verifizierenden Elemente dar. Für Ihre spezifische Sicherheitsanwendung bestehen möglicherweise zusätzliche Sicherheitsanforderungen, für die in den Checklisten genügend Platz gelassen wurde.

**TIPP** Kopieren Sie die Checklisten und bewahren Sie diese Seiten für die zukünftige Verwendung sorgfältig auf.

# Checkliste für GuardLogix-Steuerungssystem

| **Checkliste für GuardLogix-System** | | | | |
|---|---|---|---|---|
| **Unternehmen** | | | | |
| **Standort** | | | | |
| **Definition der Sicherheitsfunktion** | | | | |
| **Nummer** | **Systemanforderungen** | **Erfüllt** | | **Kommentar** |
| | | **Ja** | **Nein** | |
| 1 | Verwenden Sie nur die unter SIL 3-zertifizierte GuardLogix-Komponenten auf Seite 16 und auf der Website http://www.rockwellautomation.com/products/certification/safety/ aufgeführten Komponenten mit der entsprechenden Firmware-Version? | ☐ | ☐ | |
| 2 | Haben Sie die Sicherheitsreaktionszeit des Systems für jede Sicherheitskette berechnet? | ☐ | ☐ | |
| 3 | Beinhaltet die Reaktionszeit des Systems sowohl den benutzerdefinierten Überwachungszeitraum des Sicherheits-Task-Programms (Software-Überwachungszeitraum) als auch die Geschwindigkeit/Periode der Sicherheits-Task? | ☐ | ☐ | |
| 4 | Steht die Systemreaktionszeit in einem angemessenen Verhältnis zur Toleranzzeit des Prozesses? | ☐ | ☐ | |
| 5 | Wurden die Wahrscheinlichkeitswerte (PFD/PFH) entsprechend der Systemkonfiguration ermittelt? | ☐ | ☐ | |
| 6 | Haben Sie alle geeigneten Projektverifizierungstests durchgeführt? | ☐ | ☐ | |
| 7 | Haben Sie festgelegt, wie Ihr System auf Störungen reagiert? | ☐ | ☐ | |
| 8 | Verfügt jedes Netzwerk im Sicherheitssystem über eine eindeutige SNN? | ☐ | ☐ | |
| 9 | Sind alle CIP-Sicherheitsgeräte mit der korrekten SNN konfiguriert? | ☐ | ☐ | |
| 10 | Haben Sie eine Sicherheits-Task-Signatur erstellt? | ☐ | ☐ | |
| 11 | Haben Sie die Sicherheits-Task-Signatur für zukünftige Vergleiche hochgeladen und gespeichert? | ☐ | ☐ | |
| 12 | Haben Sie nach dem Herunterladen sichergestellt, dass die Sicherheits-Task-Signatur in der Steuerung mit der gespeicherten Sicherheits-Task-Signatur übereinstimmt? | ☐ | ☐ | |
| 13 | Haben Sie einen alternativen Mechanismus implementiert, um die Sicherheitsintegrität des Systems beizubehalten, während Sie online Bearbeitungen vornehmen? | ☐ | ☐ | |
| 14 | Haben Sie die auf den Seiten 89 und 90 aufgeführten Checklisten für den Einsatz von SIL-Eingängen und -Ausgängen berücksichtigt? | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |

## Checkliste für Sicherheitseingänge

Für die Programmierung oder Inbetriebnahme kann für jeden SIL-Eingangskanal in einem System eine eigene Checkliste ausgefüllt werden. Nur auf diese Weise ist sichergestellt, dass die Anforderungen vollständig und genau erfüllt werden. Sie können diese Checkliste auch als Dokumentation für die Anbindung externer Verdrahtung an das Anwendungsprogramm verwenden.

**Checkliste für Eingänge im GuardLogix-System**

**Unternehmen**

**Standort**

**Definition der Sicherheitsfunktion**

**SIL-Eingangskanäle**

| Nummer | Anforderungen an das Eingangsgerät | Erfüllt | | Kommentar |
|---|---|---|---|---|
| | | Ja | Nein | |
| 1 | Haben Sie die Installationsanleitungen und Vorsichtsmaßnahmen befolgt und damit die anwendbaren Sicherheitsstandards eingehalten? | ☐ | ☐ | |
| 2 | Haben Sie am System und an den Geräten Projektverifizierungstests durchgeführt? | ☐ | ☐ | |
| 3 | Werden Steuerungs-, Diagnose- und Alarmfunktionen in der Applikationslogik der Reihe nach ausgeführt? | ☐ | ☐ | |
| 4 | Haben Sie die Konfiguration jedes Geräts hochgeladen und mit der vom Konfigurationswerkzeug gesendeten Konfiguration verglichen? | ☐ | ☐ | |
| 5 | Sind die Geräte nach PLe/Cat. 4 gemäß ISO 13849-1 verdrahtet?(1) | ☐ | ☐ | |
| 6 | Haben Sie sichergestellt, dass die elektrischen Spezifikationen von Sensor und Eingang kompatibel sind? | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |

(1) Informationen zur Verdrahtung Ihres CIP Safety-E/A-Geräts finden Sie in der Produktdokumentation für das von Ihnen eingesetzte Gerät.

## Checkliste für Sicherheitsausgänge

Für die Programmierung oder Inbetriebnahme kann für jeden SIL-Ausgangskanal in einem System eine eigene Anforderungscheckliste ausgefüllt werden. Nur auf diese Weise ist sichergestellt, dass die Anforderungen vollständig und genau erfüllt werden. Sie können diese Checkliste auch als Dokumentation für die Anbindung externer Verdrahtung an das Anwendungsprogramm verwenden.

| Checkliste für Ausgänge im GuardLogix-System | | | | |
|---|---|---|---|---|
| **Unternehmen** | | | | |
| **Standort** | | | | |
| **Definition der Sicherheitsfunktion** | | | | |
| **SIL-Ausgangskanäle** | | | | |
| **Nummer** | **Anforderungen an das Ausgangsgerät** | **Erfüllt** | | **Kommentar** |
| | | **Ja** | **Nein** | |
| 1 | Haben Sie die Installationsanleitungen und Vorsichtsmaßnahmen befolgt und damit die anwendbaren Sicherheitsstandards eingehalten? | ☐ | ☐ | |
| 2 | Haben Sie für die Geräte Projektverifizierungstests durchgeführt? | ☐ | ☐ | |
| 3 | Haben Sie die Konfiguration jedes Geräts hochgeladen und mit der vom Konfigurationswerkzeug gesendeten Konfiguration verglichen? | ☐ | ☐ | |
| 4 | Haben Sie sichergestellt, dass Testausgänge nicht als Sicherheitsausgänge verwendet werden? | ☐ | ☐ | |
| 5 | Sind die Geräte nach PLe/Cat. 4 gemäß ISO 13849-1 verdrahtet?(1) | ☐ | ☐ | |
| 6 | Haben Sie sichergestellt, dass die elektrischen Spezifikationen von Ausgang und Aktor kompatibel sind? | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |

(1) Informationen zur Verdrahtung Ihres Sicherheits-E/A-Geräts finden Sie in der Produktdokumentation für das von Ihnen eingesetzte Gerät.

# Checkliste für die Entwicklung eines Programms für Sicherheitsanwendungen

Verwenden Sie die folgende Checkliste, um Sicherheit zu gewährleisten, wenn Sie ein Programm für eine Sicherheitsanwendung erstellen oder ändern.

| **Checkliste für die Entwicklung eines GuardLogix-Anwendungsprogramms** | | | | |
|---|---|---|---|---|
| **Unternehmen** | | | | |
| **Standort** | | | | |
| **Projektdefinition** | | | | |
| **Nummer** | **Anforderungen an das Anwendungsprogramm** | **Erfüllt** | | **Kommentar** |
| | | **Ja** | **Nein** | |
| 1 | Nutzen Sie Logix Designer, das Programmier-Tool für das GuardLogix-System, in der Version 21 oder höher? | ☐ | ☐ | |
| 2 | Wurden die Programmierleitlinien in Kapitel 6 bei der Erstellung des Programms für die Sicherheitsanwendung befolgt? | ☐ | ☐ | |
| 3 | Enthält das Programm für die Sicherheitsanwendung nur Kontaktplanlogik? | ☐ | ☐ | |
| 4 | Enthält das Programm für die Sicherheitsanwendung nur die in Anhang A aufgeführten Befehle, die für die Programmierung einer Sicherheitsanwendung geeignet sind? | ☐ | ☐ | |
| 5 | Unterscheidet das Programm für die Sicherheitsanwendung eindeutig zwischen Sicherheits- und Standard-Tags? | ☐ | ☐ | |
| 6 | Werden für Sicherheitsroutinen nur Sicherheits-Tags verwendet? | ☐ | ☐ | |
| 7 | Haben Sie sichergestellt, dass die Sicherheitsroutinen nicht versuchen, von Standard-Tags zu lesen oder auf diese zu schreiben? | ☐ | ☐ | |
| 8 | Haben Sie sichergestellt, dass keine Sicherheits-Tags mit Standard-Tags verbunden sind und umgekehrt? | ☐ | ☐ | |
| 9 | Sind alle Sicherheits-Tags des Ausgangs korrekt konfiguriert und mit einem physischen Ausgangskanal verbunden? | ☐ | ☐ | |
| 10 | Haben Sie sicherstellt, dass alle zugeordneten Tags in der Logik der Sicherheitsanwendung konditioniert wurden? | ☐ | ☐ | |
| 11 | Haben Sie die Prozessparameter definiert, die durch Fehlerroutinen überwacht werden? | ☐ | ☐ | |
| 12 | Haben Sie andere Sicherheits-Add-On-Befehle mit einer Befehlssignatur abgeschlossen und die Sicherheitsbefehlssignatur aufgezeichnet? | ☐ | ☐ | |
| 13 | Wurde das Programm von einem unabhängigen Sicherheitsprüfer überprüft (falls erforderlich)? | ☐ | ☐ | |
| 14 | Wurde die Überprüfung dokumentiert und unterschrieben? | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |

# Notizen:

# Sicherheitsdaten der GuardLogix-Systeme



Die folgenden Beispiele zeigen die Werte für die Versagenswahrscheinlichkeit (PFD) und die Wahrscheinlichkeit eines Ausfalls pro Stunde (PFH) für GuardLogix 1oo2 SIL 3-Systeme, die GuardLogix-E/A-Module verwenden.

Die Einsatzzeit („Mission Time") für GuardLogix-Steuerungen und Guard I/O-Module beträgt 20 Jahre.

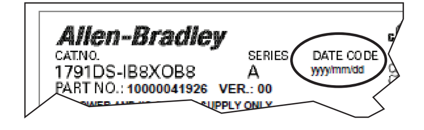
## PFD-Werte

**Tabelle 14 – Anhand des Intervalls für die Funktionsprüfung berechnete PFD**

| Bestellnummer | Beschreibung | Berechnete PFD | | | |
|---|---|---|---|---|---|
| | | 2 Jahre (17.520 Stunden) | 5 Jahre (43.800 Stunden) | 10 Jahre (87.600 Stunden) | 20 Jahre (175.200 Stunden) |
| 1756-L7*x*S und 1756-L7SP | GuardLogix-Steuerung | 5.7E-06 | 1.5E-05 | 3.5E-05 | 8.9E-05 |
| 1756-L73SXT und 1756-L7SPXT | GuardLogix XT-Steuerung | 5.7E-06 | 1.5E-05 | 3.5E-05 | 8.9E-05 |
| 1791DS-IB12 | CIP Safety-basiertes 12-Punkt-Eingangsmodul | 4.73E-07 | 1.18E-06 | 2.35E-06 | 4.71E-06(2) |
| 1791DS-IB16 | CIP Safety-basiertes 16-Punkt-Eingangsmodul | 4.11E-06 | 1.03E-05 | 2.06E-05 | 4.11E-05 |
| 1791DS-IB8XOB8 | CIP Safety-basiertes 8-Punkt-Eingangs-/ 8-Punkt-Ausgangsmodul | 4.73E-07 | 1.18E-06 | 2.35E-06 | 4.71E-06(2) |
| 1791DS-IB4XOW4 | CIP Safety-basiertes 4-Punkt-Eingangs-/ 4-Punkt Relaisausgangsmodul | 2.21E-05 | 7.05E-05 | 1.92E-04 | 5.88E-04(2) |
| 1791DS-IB8XOBV4<br>1732DS-IB8XOBV4 | CIP Safety-basiertes 8-Punkt-Eingangs-/ bipolares 4-Punkt-Ausgangsmodul | 4.16E-06 | 1.04E-05 | 2.08E-05 | 4.16E-05 |
| 1732DS-IB8 | CIP Safety-basiertes 8-Punkt-Eingangsmodul | 4.11E-06 | 1.03E-05 | 2.06E-05 | 4.11E-05 |
| 1791ES-IB16 | CIP Safety-basiertes 16-Punkt-Eingangsmodul | 4.13E-06 | 1.03E-05 | 2.06E-05 | – |
| 1791ES-IB8XOBV4 | CIP Safety-basiertes 8-Punkt-Eingangs-/ bipolares 4-Punkt-Ausgangsmodul | 4.17E-06 | 1.04E-05 | 2.09E-05 | – |
| 1734-IB8S, Serie A | CIP Safety-basiertes 8-Punkt-Eingangsmodul | 4.23E-06 | 1.06E-05 | 2.11E-05 | 4.23-05 |
| 1734-IB8S, Serie B(1) | CIP Safety-basiertes 8-Punkt-Eingangsmodul | 4.36E-06 | 1.09E-05 | 2.18E-05 | 4.36E-05 |
| 1734-OB8S, Serie A | CIP Safety-basiertes 8-Punkt-Ausgangsmodul | 4.27E-06 | 1.07E-05 | 2.13E-05 | 4.27E-05 |
| 1734-OB8S, Serie B | CIP Safety-basiertes 8-Punkt-Ausgangsmodul | 4.32E-06 | 1.08E-05 | 2.16E-05 | 4.32E-05 |
| 1734-IE4S | CIP Safety-basiertes 4-Punkt-Analog-Eingangsmodul, einkanaliger Betrieb | 4.7E-07 | 1.2E-06 | 2.4E-06 | 4.8E-06 |
| 1734-IE4S | CIP Safety-basiertes 4-Punkt-Analog-Eingangsmodul, zweikanaliger Betrieb | 3.2E-07 | 8.1E-07 | 1.6E-06 | 3.3E-06 |

(1) Diese Daten gelten für den ein- und zweikanaligen Betrieb.

(2) Die für den Zeitraum von 20 Jahren angegebenen PFD-Daten für dieses Produkt gelten nur für Produkte mit dem auf das Herstellungsdatum bezogenen Datumscode 2009/01/01 (1. Januar 2009) oder später. Sie finden den Datumscode auf dem Typenschild.



## PFH-Werte

Die nachfolgenden Daten gelten für Funktionsprüfintervalle von bis zu einschließlich 20 Jahren.

**Tabelle 15 – PFH-Berechnung**

| Bestellnummer | Beschreibung | PFH (1/Stunde) |
|---|---|---|
| 1756-L7xS und 1756-L7SP | GuardLogix-Steuerung | 1.2E-09 |
| 1756-L7xSXT und 1756-L7SPXT | GuardLogix-XT-Steuerung | 1.2E-09 |
| 1791DS-IB12 | CIP Safety-basiertes 12-Punkt-Eingangsmodul | 5.77E-11(1) |
| 1791DS-IB16 | CIP Safety-basiertes 16-Punkt-Eingangsmodul | 4.96E-10 |
| 1791DS-IB8XOB8 | CIP Safety-basiertes 8-Punkt-Eingangs-/8-Punkt-Ausgangsmodul | 5.77E-11(1) |
| 1791DS-IB4XOW4 | CIP Safety-basiertes 4-Punkt-Eingangs-/4-Punkt Relaisausgangsmodul | 9.03E-09(1) |
| 1791DS-IB8XOBV4 | CIP Safety-basiertes 8-Punkt-Eingangs-/bipolares 4-Punkt-Ausgangsmodul | 5.02E-10 |
| 1732DS-IB8XOBV4 | | |
| 1732DS-IB8 | CIP Safety-basiertes 8-Punkt-Eingangsmodul | 4.96E-10 |
| 1791ES-IB16 | CIP Safety-basiertes 16-Punkt-Eingangsmodul | 4.98E-10 |
| 1791ES-IB8XOBV4 | CIP Safety-basiertes 8-Punkt-Eingangs-/bipolares 4-Punkt-Ausgangsmodul | 5.04E-10 |
| 1734-IB8S, Serie A | CIP Safety-basiertes 8-Punkt-Eingangsmodul | 5.10E-10 |
| 1734-IB8S, Serie B | CIP Safety-basiertes 8-Punkt-Eingangsmodul | 5.27E-10 |
| 1734-OB8S, Serie A | CIP Safety-basiertes 8-Punkt-Ausgangsmodul | 5.14E-10 |
| 1734-OB8S, Serie B | CIP Safety-basiertes 8-Punkt-Ausgangsmodul | 5.20E-10 |
| 1734-IE4S | CIP Safety-basiertes 4-Punkt-Analog-Eingangsmodul, einkanaliger Betrieb<br>CIP Safety-basiertes 4-Punkt-Analog-Eingangsmodul, zweikanaliger Betrieb | 5.6E-11<br>3.9E-11 |

(1) Die für dieses Produkt angegebenen PFH-Daten gelten nur für Produkte mit dem auf das Herstellungsdatum bezogenen Datumscode 2009/01/01 (1. Januar 2009) oder später. Sie finden den Datumscode auf dem Typenschild.

# Software RSLogix 5000, ab Version 14, Beschreibung der Befehle für Sicherheitsanwendungen



## Ruhestromprinzip-System

Wenn Sie die in der Software RSLogix 5000, Version 14, enthaltenen Befehle für Sicherheitsanwendungen verwenden, werden alle Eingänge und Ausgänge auf null gesetzt, sobald ein Fehler erkannt wird. Daher sollten alle Eingänge, die mithilfe eines der Befehle für diversitäre Eingänge („Diverse Inputs“ oder „Two-hand Run Station“) überwacht werden, über Öffner-Eingänge verfügen, die durch eine Logik bedingt sind, die der Logik in Strompfad 4 in Kontaktplanlogik – Beispiel 2 und Kontaktplanlogik – Beispiel 3 auf den Seiten 98 und 99 ähnlich ist. Welche Logik genau erforderlich ist, hängt sowohl von der Anwendung als auch vom Eingangsgerät ab. Allerdings muss die Logik den sicheren Zustand 1 für den Öffnereingang, der durch einen dieser Befehle überwacht wird, erstellen.

## Verwenden von Verbindungsstatusdaten zur programmatischen Einleitung einer Störung

Die folgenden Diagramme sind Beispiele für die Kontaktplanlogik, die zum Verriegeln und Zurücksetzen eines E/A-Moduls bei einem Ausfall erforderlich ist. Die Beispiele zeigen die Logik, die für ein Modul, das nur über Eingänge verfügt, bzw. für ein Modul mit Ein- und Ausgängen erforderlich ist. In den Beispielen wird die Funktion „Combined Status“ (Kombinierter Zustand) der E/A-Module verwendet, die den Status aller Eingangskanäle in einer einzigen booleschen Variablen darstellt. Mit einer weiteren booleschen Variablen wird der Zustand aller Ausgangskanäle dargestellt. Mit diesem Konzept kann der Umfang der erforderlichen E/A-Konditionierungslogik reduziert werden und die Logik geforced werden, alle Eingangs- oder Ausgangskanäle am betroffenen Modul zu deaktivieren.

Bestimmen Sie anhand der Abbildung Ablaufdiagramm zum Verriegeln und Zurücksetzen eines Eingangs auf Seite 96, welche Strompfade der Logik für verschiedene Anwendungssituationen erforderlich sind. Kontaktplanlogik – Beispiel 1 zeigt Logik, die die tatsächlichen Eingangs-Tag-Variablen überschreibt, während ein Fehlerzustand vorliegt. Wenn der tatsächliche Eingangszustand zur Fehlerbehebung erforderlich ist, während der fehlerhafte Eingang verriegelt ist, dann verwenden Sie die Logik in Kontaktplanlogik – Beispiel 2. Diese Logik verwendet interne Tags, die die in der Anwendungslogik zu verwendenden

Eingänge darstellen. Während der Eingang verriegelt ist, werden die internen Tags in den sicheren Zustand gesetzt. Während der Eingang nicht verriegelt ist, werden die tatsächlichen Eingangswerte in die internen Tags kopiert.

Bestimmen Sie anhand der Abbildung Ablaufdiagramm zum Verriegeln und Zurücksetzen eines Ausgangs, welche Strompfade der Kontaktplanlogik in Kontaktplanlogik – Beispiel 3 auf Seite 99 erforderlich sind.

**Abbildung 22 – Ablaufdiagramm zum Verriegeln und Zurücksetzen eines Eingangs**

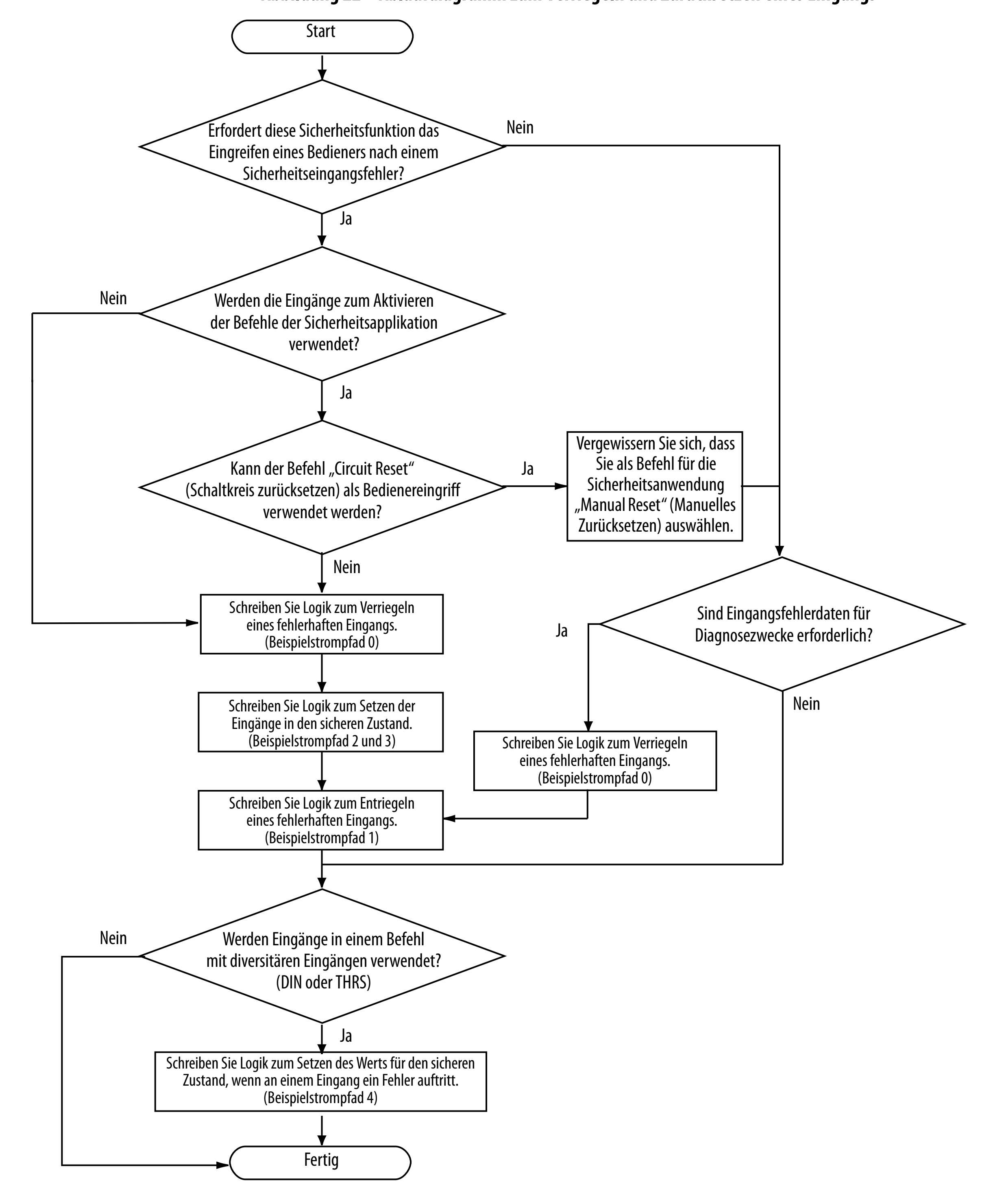


**Abbildung 23 – Kontaktplanlogik – Beispiel 1**

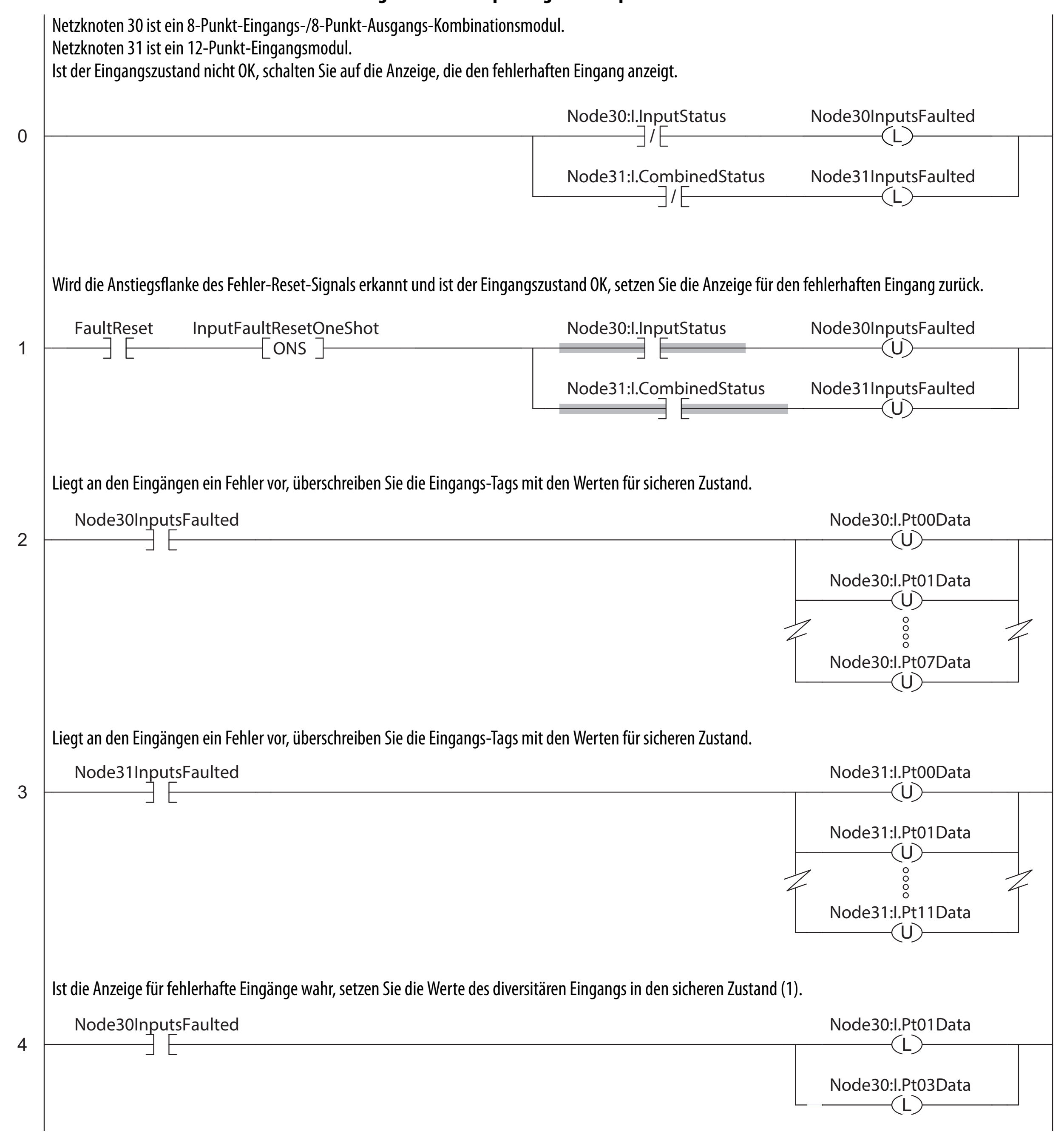


**Abbildung 24 – Kontaktplanlogik – Beispiel 2**

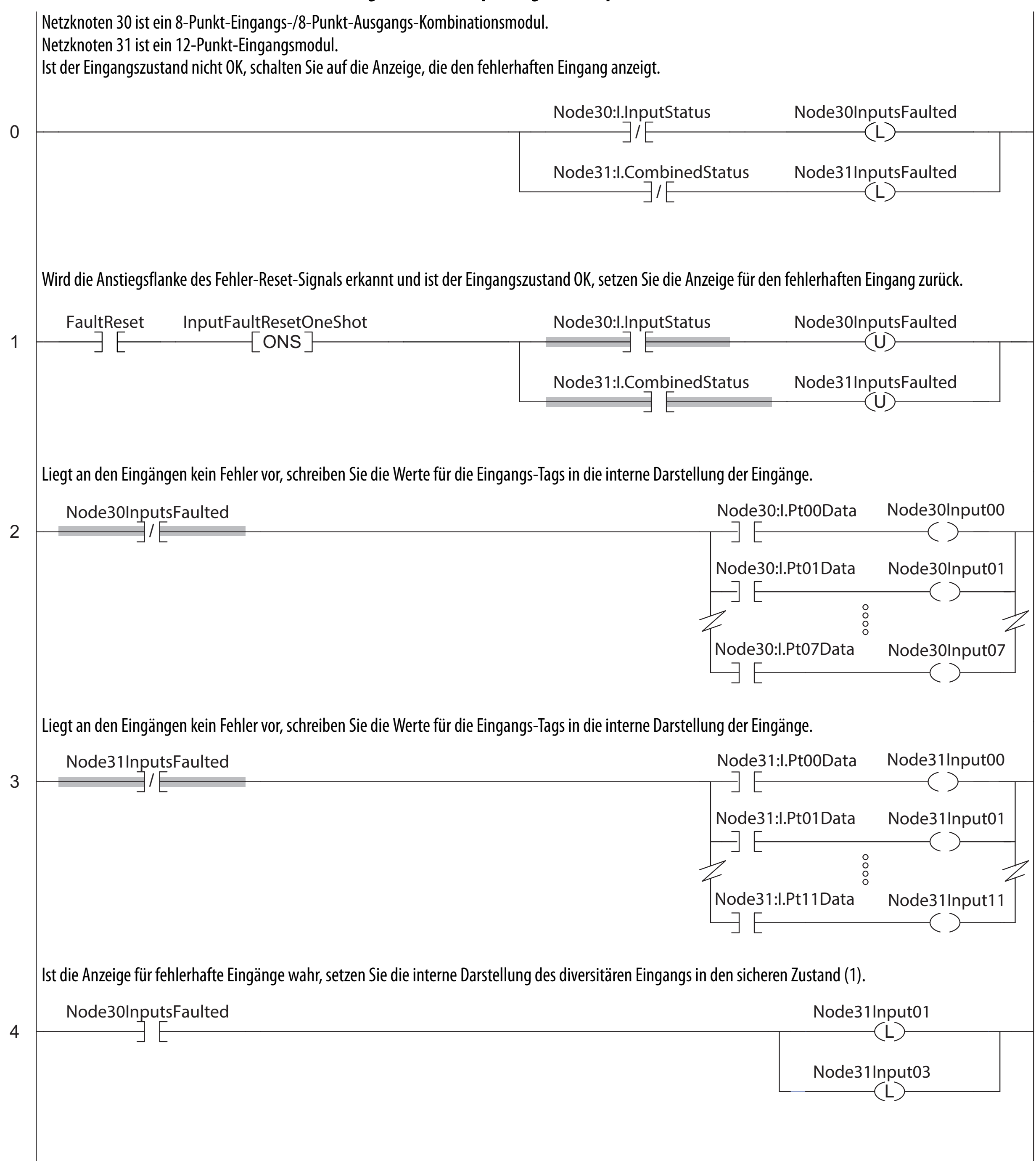


**Abbildung 25 – Ablaufdiagramm zum Verriegeln und Zurücksetzen eines Ausgangs**

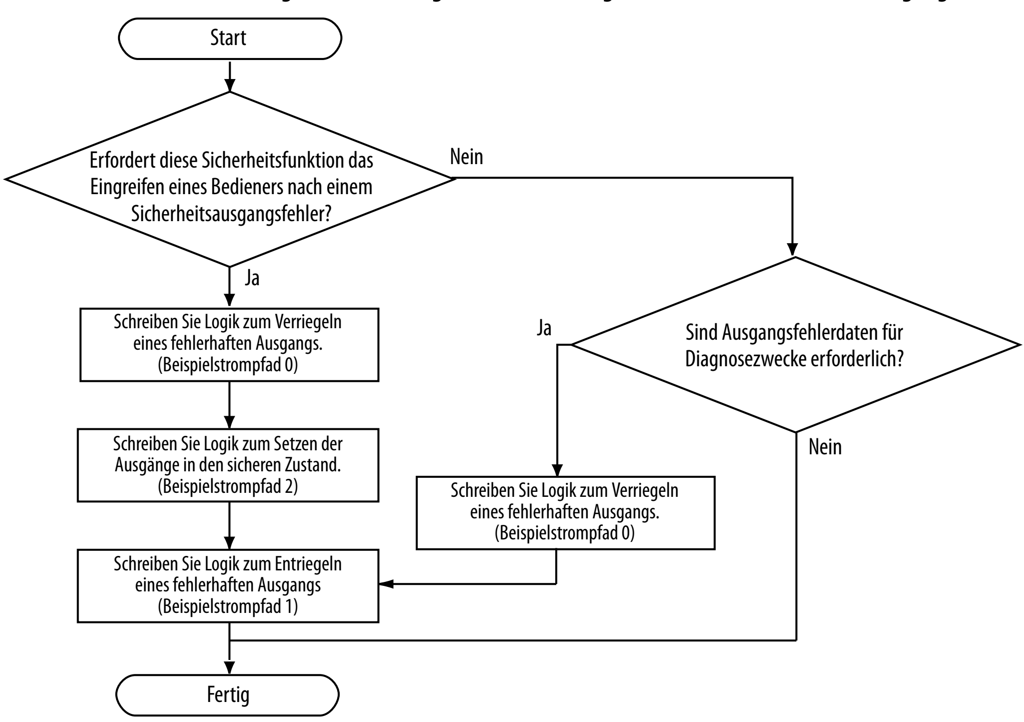
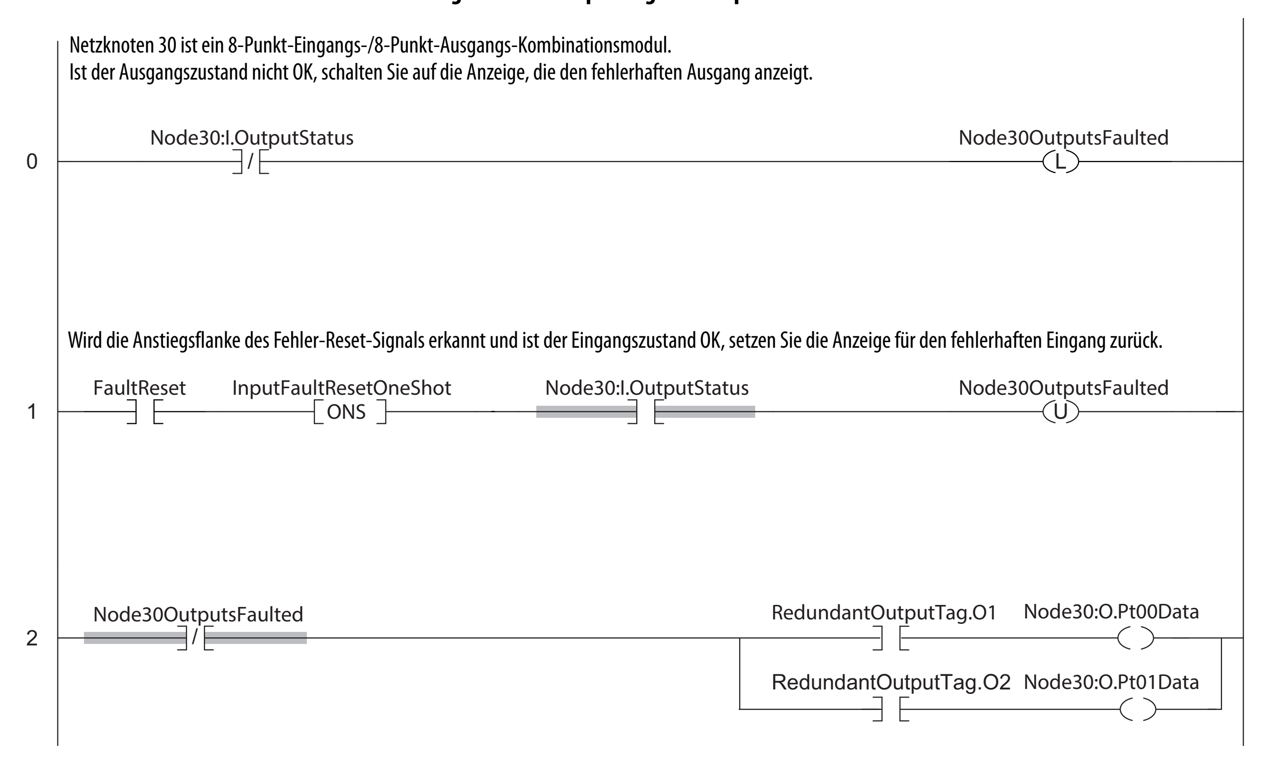



**Abbildung 26 – Kontaktplanlogik – Beispiel 3**



# Notizen:

# Verwendung von 1794 FLEX I/O-Modulen und 1756 SIL 2-Eingängen und -Ausgängen mit 1756 GuardLogix-Steuerungen zur Einhaltung der EN 50156

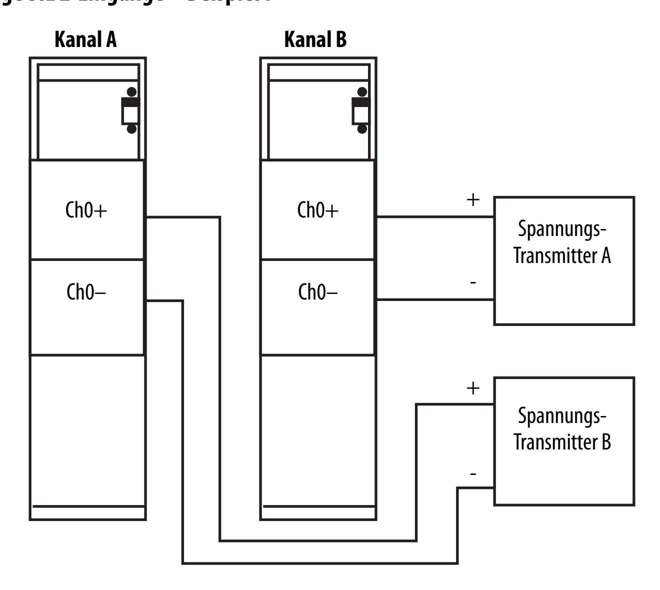


Zur Einhaltung der behördlichen Bestimmungen ist in bestimmten sicherheitstechnischen Anwendungen eine Zweikanalkonfiguration erforderlich; hierzu gehören auch brennerbezogene Sicherheitsfunktionen. Die folgenden Beispiele sollen als Leitlinien zur Einhaltung der Anforderungen der EN50156 an SIL 2-Zweikanalkonfigurationen mit Testintervallen von 1 und 2 Jahren dienen.

## Zweikanalige SIL 2-Eingänge (Standardseite der GuardLogix-Steuerungen)

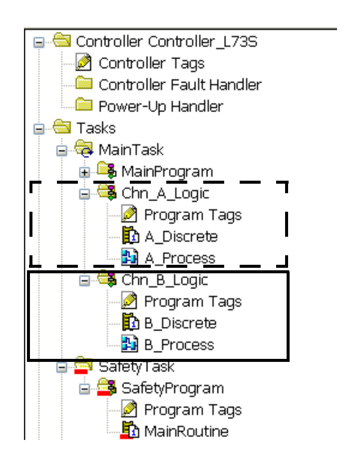
Sie müssen eine klare und einfach zu identifizierende Trennung zwischen beiden Eingangskanälen implementieren und alle SIL 2-Anforderungen erfüllen, wie sie im Referenzhandbuch „Using ControlLogix in SIL 2 Applications“, Publikation 1756-RM001, definiert sind.

**Abbildung 27 – Zweikanalige SIL 2-Eingänge – Beispiel F**



*SIL 2-Eingangsdaten*

Achten Sie stets darauf, dass die Eingangsdaten von Kanal A und Kanal B voneinander getrennt bleiben. Dieses Beispiel zeigt eine Methode, wie die Daten von Kanal A und Kanal B in Ihrer Anwendung voneinander getrennt werden können.

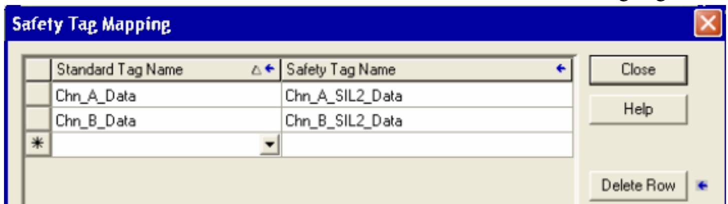



Halten Sie alle Vorschriften ein, die für die 1756-E/A-Module und die 1794 FLEX™-E/A-Module im Referenzhandbuch „Using ControlLogix in SIL 2 Applications Safety“, Publikation 1756-RM001, aufgeführt sind.

| | |
|---|---|
| **WICHTIG** | Implementieren Sie keine sicherheitsspezifischen Funktionen in diese Routinen. Die Sicherheitsbewertung muss in der 1756 GuardLogix Sicherheits-Task vorgenommen werden. |

*SIL 2-Daten in die Sicherheits-Task übertragen*

Verwenden Sie die Zuordnungsfunktionalität für Sicherheits-Tags in der Anwendung Logix Designer, um die SIL 2-Sicherheitsdaten von Kanal A und Kanal B in die GuardLogix-Sicherheits-Task zu übertragen. Die hier verwendeten Tag-Namen dienen nur als Beispiele. Implementieren und befolgen Sie Namenskonventionen, die sich für Ihre Anwendung eignen.




| | |
|---|---|
| **TIPP** | Um die Zuordnungsfunktion für Sicherheits-Tags zu verwenden, wählen Sie in der Anwendung Logix Designer im Menü „Logic“ (Logik) die Option „Map Safety Tags“ (Sicherheits-Tags zuordnen) aus. |

## Verwendung von SIL 3-Guard I/O-Ausgangsmodulen mit SIL 2-Ausgängen

Beachten Sie folgende Leitlinien zu SIL 2-Ausgängen:

- Guard I/O-Ausgangsmodule, die für SIL 2-Sicherheitsausgänge verwendet werden, müssen für den Zweikanalbetrieb konfiguriert werden.
- Alle Guard I/O-Ausgangsmodule sind für die Verwendung in SIL 2-Anwendungen zugelassen.
  – 1732DS-IB8XOBV4
  – 1791ES-IB8XOBV4
  – 1791DS-IB8XOBV4, 1791ES-IB8XOBV4
  – 1791DS-IB4XOW4
  – 1791DS-IB8XOB8
  – 1734-OB8S

## Verwendung von 1756 oder 1794 SIL 2-Ausgangsmodulen mit SIL 2-Ausgängen

Wenn Sie diese für SIL 2 ausgelegten Module verwenden, müssen Sie Ihre SIL 2-Sicherheitsausgänge als von GuardLogix produzierte Sicherheits-Tags konfigurieren, um die Anforderungen der EN 50156 an Zweikanalkonfigurationen zu erfüllen.

Erzeugen Sie produzierte Sicherheits-Tags mit den SIL 2-Ausgängen, die Ihre Anwendung erfordert. Die produzierten/konsumierten GuardLogix-Sicherheits-Tags erfordern, dass das erste Glied der Diagnose zugewiesen wird. Beim ersten Glied einer produzierten/konsumierten Sicherheitsverbindung muss es sich um einen Datentyp mit der Bezeichnung CONNECTION_STATUS handeln. Dieses Beispiel zeigt ein SIL 2-Tag mit zwei ganzzahligen (INT) und zwei booleschen (BOOL) Gliedern. Verwenden Sie diese SIL 2-Sicherheits-Tags, um die SIL 2-Ausgänge des 1756- oder 1794-Moduls direkt zu steuern.

| Name | Alias For | Base Tag | Data Type | Class | Description | External Access | Constant | Style |
|---|---|---|---|---|---|---|---|---|
| ⊟-SIL2_Outputs | | | SIL_2_Produced | Safety | | Read/Write | ☐ | |
| ⊞-SIL2_Outputs.Connection_Status | | | CONNECTION_STA | Safety | | Read/Write | | |
| ⊞-SIL2_Outputs.SIL2_TempA | | | INT | Safety | | Read/Write | | Decimal |
| ⊞-SIL2_Outputs.SIL2_TempB | | | INT | Safety | | Read/Write | | Decimal |
| SIL2_Outputs.SIL2_Valve1 | | | BOOL | Safety | | Read/Write | | Binary |
| SIL2_Outputs.SIL2_Valve2 | | | BOOL | Safety | | Read/Write | | Binary |

**TIPP** In diesem Beispiel wird kein Consumer für das produzierte Tag gezeigt. Wenn Sie keinen Consumer konfigurieren, wird für den Verbindungsstatus ein Fehler ausgegeben. Allerdings brauchen Sie den Verbindungsstatus des produzierten Tags in dieser Konfigurationsart nicht zu überwachen, weshalb der Fehler kein Problem darstellt.

Halten Sie alle Vorschriften ein, die für die 1756-E/A-Module und die 1794 FLEX-E/A-Module im Referenzhandbuch „Using ControlLogix in SIL 2 Applications Safety“, Publikation 1756-RM001, aufgeführt sind.

## Sicherheitsfunktionen in der 1756 GuardLogix-Sicherheits-Task

Beachten Sie folgende Leitlinien, um SIL 2- und SIL 3-Sicherheitsfunktionen in der Sicherheits-Task zu verwenden:

- Es können alle verfügbaren Befehle der Sicherheitsanwendung verwendet werden.
- Die SIL CL3-Sicherheitseingangsmodule (d. h. Guard I/O-Module) können mit einer Einkanalkonfiguration für SIL 2-Sicherheitsfunktionen verwendet werden.
- Die Verwendung der Sicherheits-Task-Signatur und die Sicherheits-verriegelung der Anwendung werden empfohlen.

| | |
|---|---|
| **WICHTIG** | Sie dürfen SIL 2-Daten nicht zur direkten Steuerung eines SIL 3-Ausgangs verwenden. |

# Glossar

In diesem Handbuch werden die folgenden Begriffe und Abkürzungen verwendet. Definitionen zu hier nicht aufgeführten Begriffen finden Sie im „Industrial Automation Glossary“ von Allen-Bradley, Publikation AG-7.1.

**Add-On-Befehl** Ein Befehl, den Sie optional zum Logix-Befehlssatz erstellen. Einmal definiert kann ein Add-On-Befehl wie jeder andere Logix-Befehl verwendet und in einer Vielzahl von Projekten genutzt werden. Ein Add-On-Befehl besteht aus Parametern, lokalen Tags, Logikroutine und optionalen Scan-Modus-Routinen.

**Anstehende Bearbeitung** Eine Änderung an einer Routine, die in der Anwendung Logix Designer vorgenommen wurde, aber der Steuerung noch nicht durch Übernahme der Änderung mitgeteilt wurde.

**Bearbeitungen assemblieren** Der Anwender führt diese Aktion aus, wenn er Online-Bearbeitungsänderungen am Steuerprogramm vorgenommen hat und diese Änderungen dauerhaft festlegen will, da er die Änderungen testen, ihren Test aufheben oder sie löschen kann.

**Bearbeitungen löschen** Der Anwender führt diese Aktion aus, um alle nicht assemblierten Online-Bearbeitungsänderungen zu verwerfen.

**Befehle für die Sicherheitsanwendung** Sicherheitsbefehle, die sicherheitstechnische Funktionalität bereitstellen. Sie wurden nach SIL 3 zur Verwendung in Sicherheitsroutinen zertifiziert.

**Befehlssignatur** Die Befehlssignatur besteht aus einer ID-Nummer und einem Datums-/Zeitstempel, der den Inhalt der Add-On-Befehlsdefinition zu einem bestimmten Zeitpunkt identifiziert.

**Gültige Verbindung** Sicherheitsverbindung ist offen und aktiv sowie fehlerfrei.

**Konfigurationssignatur** Eine eindeutige Zahl, die die Konfiguration eines Geräts identifiziert. Die Konfigurationssignatur besteht aus einer ID-Nummer, Datum und Uhrzeit.

**Korrigierbarer Fehler** Ein Fehler, der bei ordnungsgemäßer Handhabung durch die Implementierung der von der Steuerung bereitgestellten Mechanismen zur Fehlerhandhabung keine Beendigung der Anwenderlogikausführung erzwingt.

**Nicht korrigierbarer Sicherheitsfehler** Ein Fehler, durch den die gesamte Verarbeitung der Sicherheits-Task beendet wird und der zum Neustart der Sicherheits-Task externe Anwendereingriffe erfordert – auch wenn er durch die von der Sicherheitssteuerung bereitgestellten und vom Anwender implementierten Mechanismen zur Fehlerhandhabung ordnungsgemäß gehandhabt wird.

**Nicht korrigierbarer Steuerungsfehler** Ein Fehler, der das Ende der gesamten Verarbeitung erzwingt und das Aus- und Wiedereinschalten der Steuerspannung erforderlich macht. Das Anwenderprogramm bleibt nicht erhalten und muss neu heruntergeladen werden.

**online** Situation, in der der Anwender das Programm in der Steuerung überwacht/ändert.

**Partnerschaft** Die Primärsteuerung und der Sicherheitspartner müssen beide vorhanden sein und Hard- sowie Firmware müssen kompatibel sein, damit die Partnerschaft eingerichtet werden kann.

**Periodische Task** Eine Task (Aufgabe), die vom Betriebssystem in einer sich wiederholenden Zeitperiode ausgelöst wird. Nach einer definierten Zeit wird die Aufgabe ausgelöst und deren Programme werden ausgeführt. Daten und Ausgänge, die von den Programmen in der Aufgabe gebildet wurden, behalten ihre Werte bis zur nächsten Ausführung der Aufgabe bei oder bis sie von einer anderen Aufgabe manipuliert werden. Periodische Tasks unterbrechen immer die kontinuierliche Task.

**Primärsteuerung** Der Prozessor einer Steuerung mit zwei Prozessoren, der die Funktionen der Standardsteuerung ausführt und mit dem Sicherheitspartner hinsichtlich der Ausführung sicherheitsgerichteter Funktionen kommuniziert.

**Requested Packet Interval (RPI)** Bei der Kommunikation über ein Netzwerk umfasst dieser Wert die maximale Zeit zwischen aufeinander folgender Produktion von Eingangsdaten.

**Routine** Ein Befehlssatz logischer Kommandos in einer einzigen Programmiersprache, wie einem Kontaktplan. Routinen stellen ausführbaren Code für das Projekt in einer Steuerung bereit. Jedes Programm verfügt über eine Hauptroutine. Es können auch optionale Routinen spezifiziert werden.

**Sicherheits-Add-On-Befehl** Ein Add-On-Befehl, der die Befehle einer Sicherheitsanwendung verwenden kann. Zusätzlich zur Befehlssignatur, die für Add-On-Befehle hoher Integrität verwendet wird, bieten Sicherheits-Add-On-Befehle eine SIL 3-Sicherheitsbefehlssignatur zur Verwendung in sicherheitstechnischen Funktionen.

**Sicherheits-E/A** Sicherheits-E/A verfügen über die meisten Eigenschaften der Standard-E/A, außer dass sie Mechanismen besitzen, die nach SIL 3 zertifiziert sind, um Datenintegrität sicherzustellen.

**Sicherheits-Tags** Ein Sicherheits-Tag verfügt über alle Eigenschaften eines Standard-Tags, wobei die GuardLogix-Steuerung Mechanismen bereitstellt, die nach SIL 3 zertifiziert sind, um die Integrität der verknüpften Daten zu schützen. Sie können im Programmbereich oder Steuerungsbereich liegen.

**Sicherheits-Task** Eine Sicherheits-Task verfügt über alle Eigenschaften einer Standard-Task, außer dass sie nur in einer GuardLogix-Steuerung gültig ist und nur Sicherheitsprogramme planen kann. Es kann nur eine Sicherheits-Task in einer GuardLogix-Steuerung existieren. Die Sicherheits-Task muss eine periodische/zeitgesteuerte Task sein.

**Sicherheits-Task-Periode** Die Periode, mit der die Sicherheits-Task ausgeführt wird.

**Sicherheits-Task-Reaktionszeit** Die Summe von Sicherheits-Task-Periode und Sicherheits-Task-Überwachungszeitraum. Diese Zeit stellt die längstmögliche Verzögerung einer bei der GuardLogix-Steuerung eingehenden Eingangsänderung dar, bis der verarbeitete Ausgang für die produzierende Verbindung zur Verfügung steht.

**Sicherheits-Task-Signatur** Ein Wert, der von der Firmware berechnet wird und die Logik sowie Konfiguration des Sicherheitssystems eindeutig repräsentiert. Die Signatur dient dazu, die Integrität des Sicherheitsanwendungsprogramms beim Herunterladen auf die Steuerung zu verifizieren.

**Sicherheits-Task-Überwachungszeitraum** Die maximal zulässige Zeit ab dem Start der Sicherheits-Task-Ausführung bis zu ihrem Abschluss. Wird der Sicherheits-Task-Überwachungszeitraum überschritten, löst dies einen nicht korrigierbaren Sicherheitsfehler aus.

**Sicherheitsbefehlssignatur** Bei der Sicherheitsbefehlssignatur handelt es sich um eine ID-Nummer, die die Ausführungsmerkmale des Sicherheits-Add-On-Befehls identifiziert. Die Signatur dient dazu, die Integrität des Sicherheits-Add-On-Befehls beim Herunterladen auf die Steuerung zu verifizieren.

**Sicherheitskomponente** Alle Objekte, Tasks, Programme, Routinen, Tags, Module usw., die als sicherheitsgerichtete Elemente gekennzeichnet sind.

**Sicherheitsnetzwerknummer (SNN – Safety Network Number)** Identifiziert ein Netzwerk eindeutig in allen Netzwerken im Sicherheitssystem. Der Endnutzer ist für die Zuordnung einer eindeutigen Nummer zu jedem Sicherheitsnetzwerk oder Sicherheitsteilnetz in einem System verantwortlich. Die Sicherheitsnetzwerknummer stellt einen Teil der eindeutigen Netzknoten-ID (Unique Node Identifier, UNID) dar.

**Sicherheitspartner** Der Prozessor einer Steuerung mit zwei Prozessoren, der mit der Primärsteuerung hinsichtlich der Ausführung sicherheitsgerichteter Funktionen zusammenarbeitet.

**Sicherheitsprogramm** Ein Sicherheitsprogramm verfügt über alle Eigenschaften eines Standardprogramms, lässt sich aber nur in einer Sicherheits-Task planen. Das Sicherheitsprogramm besteht aus null oder mehr Sicherheitsroutinen. Es kann keine Standardroutinen oder Standard-Tags enthalten.

**Sicherheitsprotokoll CIP Safety** Das Sicherheitsprotokoll CIP Safety stellt ein Verfahren zur Netzwerkkommunikation dar, das für den Transport von Daten mit hoher Integrität ausgelegt und zertifiziert ist.

**Sicherheitsroutine** Eine Sicherheitsroutine verfügt über alle Eigenschaften einer Standardroutine, ist aber nur in einem Sicherheitsprogramm gültig und besteht aus einem oder mehreren für Sicherheitsanwendungen geeigneten Befehlen. (Eine Liste der Befehle für Sicherheitsanwendungen und der Logix-Standardbefehle, die in der Logik einer Sicherheitsroutine verwendet werden können, finden Sie in Anhang A.)

**Standardkomponente** Alle Objekte, Tasks, Programme usw., die als **nicht** sicherheitsgerichtete Elemente gekennzeichnet sind.

**Standardsteuerung** In der vorliegenden Dokumentation wird „Standardsteuerung" als Oberbegriff für eine ControlLogix-Steuerung verwendet.

**Symbolische Adressierung** Ein Adressierungsverfahren, das eine ASCII-Auslegung des Tag-Namens liefert.

**Systemreaktionszeit** Die längstmögliche Zeit zwischen Eingang eines sicherheitsgerichteten Ereignisses im System oder Störung in einem System und dem Zeitpunkt, an dem sich das System im sicheren Zustand befindet. Die Systemreaktionszeit umfasst Sensor- und Aktorreaktionszeiten sowie die Steuerungsreaktionszeit.

**Task** Ein Scheduling-Mechanismus zur Ausführung eines Programms. Eine Task stellt Scheduling- und Prioritätsinformationen für ein Programm oder mehrere Programme bereit, die basierend auf bestimmten Kriterien ausgeführt werden. Sobald eine Task ausgelöst (aktiviert) ist, werden alle der Task zugeordneten (geplanten) Programme in der Reihenfolge ausgeführt, in der sie im Controller Organizer (Steuerungsorganisator) angezeigt werden.

**Timeout-Multiplikator** Dieser Wert bestimmt die Anzahl von Nachrichten, die verloren gehen dürfen, bevor ein Verbindungsfehler deklariert wird.

**Überlappung** Wenn eine Task (periodisch oder ereignisgesteuert) ausgelöst wird, während die Task, ausgelöst durch den vorherigen Trigger, noch ausgeführt wird.

## Ziffern



## A



## B



## C



## D



## E



## F

## T



## U



## V



## W



## X



## Z

## Kundendienst von Rockwell Automation

Rockwell Automation bietet Ihnen über das Internet Unterstützung bei der Verwendung seiner Produkte. Unter http://www.rockwellautomation.com/support finden Sie technische Hinweise und Applikationsbeispiele, Beispielcode und Links zu Software-Service-Packs. In unserem Support Center unter https://rockwellautomation.custhelp.com/ finden Sie außerdem Software-Updates, Support-Chats und Foren, technische Informationen, Antworten auf häufig gestellte Fragen und Sie können sich für Benachrichtigungen über Produkt-Updates anmelden.

Darüber hinaus bieten wir mehrere Support-Programme für die Installation, Konfiguration und Fehlerbehebung an. Wenn Sie weitere Informationen wünschen, wenden Sie sich bitte an den für Sie zuständigen Distributor oder Rockwell Automation-Mitarbeiter. Sie können uns auch gerne auf unserer Website http://www.rockwellautomation.com/services/online-phone besuchen.

### Unterstützung bei der Installation

Wenn innerhalb von 24 Stunden nach der Installation ein Problem auftritt, lesen Sie bitte die Informationen in diesem Handbuch. Außerdem können Sie sich an den Kundendienst wenden, wenn Sie Unterstützung bei Einrichtung und Inbetriebnahme Ihres Produktes benötigen.

| | |
|---|---|
| USA oder Kanada | 1.440.646.3434 |
| Außerhalb der USA oder Kanada | Nutzen Sie den Worldwide Locator unter http://www.rockwellautomation.com/rockwellautomation/support/overview.page oder wenden Sie sich an den für Sie zuständigen Mitarbeiter von Rockwell Automation. |

### Rückgabeverfahren bei neuen Produkten

Rockwell Automation testet alle Produkte, um sicherzustellen, dass sie beim Verlassen des Werks voll funktionsfähig sind. Sollte trotzdem eines Ihrer Produkte nicht ordnungsgemäß arbeiten und an Rockwell Automation zurückgesendet werden müssen, dann gehen Sie dazu bitte wie im Folgenden beschrieben vor.

| | |
|---|---|
| USA | Wenden Sie sich an Ihren Distributor. Sie müssen Ihrem Distributor eine Kundendienst-Bearbeitungsnummer angeben (diese erhalten Sie über die oben genannte Telefonnummer), damit das Rückgabeverfahren abgewickelt werden kann. |
| Außerhalb der USA | Bitte wenden Sie sich bei Fragen zum Rückgabevorgang an den für Sie zuständigen Mitarbeiter von Rockwell Automation. |

## Feedback zur Dokumentation

Ihre Kommentare helfen uns dabei, Ihre Dokumentationsanforderungen noch besser zu erfüllen. Falls Sie Verbesserungsvorschläge zu diesem Dokument haben, füllen Sie bitte das folgende Formular aus: Publikation RA-DU002, verfügbar unter http://www.rockwellautomation.com/literature/.

Rockwell Automation verwaltet aktuelle Informationen zu Produktumgebungen auf seiner Website unter http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page.

**www.rockwellautomation.com**

**Hauptverwaltung für Antriebs-, Steuerungs- und Informationslösungen**

Amerika: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204 USA, Tel: +1 414 382 2000, Fax: +1 414 382 4444
Europa/Naher Osten/Afrika: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgien, Tel: +32 2 663 0600, Fax: +32 2 663 0640
Asien/Australien/Pazifikraum: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, China, Tel: +852 2887 4788, Fax: +852 2508 1846

Deutschland: Rockwell Automation GmbH, Parsevalstraße 11, 40468 Düsseldorf, Tel: +49 (0)211 41553 0, Fax: +49 (0)211 41553 121
Schweiz: Rockwell Automation AG, Industriestrasse 20, CH-5001 Aarau, Tel: +41(62) 889 77 77, Fax: +41(62) 889 77 11, Customer Service – Tel: 0848 000 277
Österreich: Rockwell Automation, Kotzinastraße 9, A-4030 Linz, Tel: +43 (0)732 38 909 0, Fax: +43 (0)732 38 909 61